|  |
| --- |
| Toshiba |
| JED Consulting LLC |
| Security Approach to Cyber Security |
|  |
| **John E. Donnelly III** |
| **11/12/2016** |

|  |
| --- |
| This document is brief Business Plan and Product description about JED Consulting Services LLC. The contents are proprietary and confidential company information that is considered intellectual property that is not to be transmitted or recorded in any means without the express written permission of the author. |

**JED Security Approach to Cyber Security 2016**

### Security & Risk Management

Protecting information confidentiality is a critical security objective for every organization. Starting with a good understanding of the business, an organization must weave IT security and IT risk management into the executive levels of business planning. IT security objectives must be defined for the organization as a whole and fall within the following categories: integrity, availability, confidentiality, use control and accountability. The objectives provide the criteria used to determine whether the architecture is appropriate for the given task. John has an established methodology for assessing and developing comprehensive IT security architectures and deployment strategies, including identity and access management (IAM) architectures. Our focus is on people, processes and technology, including benchmarking your IT security strategy and cost models.

#### UNDERSTANDING

##### We understand the key issues you are facing.

* Sensitive data loss prevention is one of the key areas of focus in light of industry and government regulations and the potential for large-scale negative publicity.
* A proper business case with financial analysis is necessary to spearhead and fund an IT security or IAM project successfully.
* Outmoded user account management and access controls constrict your ability to know and restrict who has access to what.
* Governance frameworks for IT security and IAM are necessary to be successful over the longer term.
* Vendor hype and vaporware leads to paralysis by analysis, FUD or the implementation of the wrong set of solutions.

#### CAPABILITIES

##### We have the data, tools and capabilities to help

* Seasoned experts who apply best practices, business models and proven technologies to solve today’s most pressing IT security challenges
* In-depth methodologies for assessing and developing the right strategy and architecture for your company in your specific industry
* Workshop and training offerings to educate stakeholders and arm them with the information necessary to make key organizational, process and architecture decisions
* Cost, price and process benchmarks to compare your IT security strategy and performance to industry peers
* Architecture and vendor recommendations for provisioning, access control, roles, single sign-on, identity data integration, audit and certificate management
* Assessment and recommendations for IT security management, policy, standards and procedures, legal considerations, encryption usage, training and education, security awareness, organizational issues, documentation, protection audit, protection testing, technical safeguards, personnel issues, physical security, incident response

**Dear Senior IT Executives**

**As a CIO and senior IT leader, you need actionable advice to drive digital to the core of your products, processes and talent. But you also need to prepare for disruptive trends that can help you deliver long-term business benefits. Our theme: “Leadership: 360. Drive Digital to the Core”, will help you see further, explore deeper and to discover how to make digital a core competence for you and your organization.**

**Since 1989, John has been helping create an environment that realistically and cost effectively protects networks while maintaining a balance of productivity and operational effectiveness.**

**John has developed a suite of services to support your entire cybersecurity lifecycle. This includes program development, education and training, plus Discovery Log Analysis Service and Digital Forensic Services.**

**We consider ourselves an extension of your team. Our #1 goal is to help ensure that your organization is fully trained, compliant, and prepared for evolving cybersecurity threats.**

**Contact us today to learn how we can help you enrich your existing information security program, champion cybersecurity, and transition your organization**

**At JED, we believe in challenging the established mindsets, approaches, and product categories in the information security industry. Every service we deliver to the market is based on a core set of principles grounded in the major paradigm shifts in play and the implications that they have for our customers. And we live by values that support our actions every day in everything we do.**

1. **Do the right thing- by our customers, employees, and stakeholders. We think long-term but take action with a sense of urgency.**
2. **What we do matters. Our work makes a difference in the world.**
3. **We give a damn. About our customers, about what we’re doing, about each other. We are in this together.**

#### We are a fun company. We are building cool products and services with technical insight that help our customers solve meaningful problems.

|  |  |
| --- | --- |
| Table 1 2016 Hot Topics | Please rank top 10 security topics |
| Enabling a safer cloud | Regulatory changes on global business operations |
| Governance, risk and compliance | Cybersecurity Frameworks |
| Recovery from a targeted cyberattack | Mobile security for digital business |
| Security and risk strategy | Transitioning from recovery to resilience |
| * Crisis/incident command and management | * Emerging security technologies |
| * Internet of Things, network and endpoint security challenges | * Optimizing security information and event management and threat intelligence tool |

**Information is a key resource for all enterprises**, and from the time that information is created to the moment that it is destroyed, technology plays a significant role. Information technology is increasingly advanced and has become pervasive in enterprises and in social, public and business environments.

As a result, today, more than ever, enterprises and their executives strive to:

* Maintain high-quality information to support business decisions.
* Generate business value from IT-enabled investments, i.e., achieve strategic goals and realise business benefits through effective and innovative use of IT.
* Achieve operational excellence through the reliable and efficient application of technology.
* Maintain IT-related risk at an acceptable level.
* Optimize the cost of IT services and technology.
* Comply with ever-increasing relevant laws, regulations, contractual agreements and policies.

Over the past decade, the term ‘governance’ has moved to the forefront of business thinking in response to examples demonstrating the importance of good governance and, on the other end of the scale, global business mishaps.

Successful enterprises have recognized that the board and executives need to embrace IT like any other significant part of doing business. Boards and management—both in the business and IT functions—must collaborate and work together, so that IT is included within the governance and management approach. In addition, legislation is increasingly being passed and regulations implemented to address this need.

COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. Simply stated, it helps enterprises create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use. COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders. COBIT 5 is generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

**Our mission is to help customers around the world build essential security capabilities to protect their most valuable assets from cyber threats. We utilize award winning products, to help organizations effectively detect, investigate, and respond to advance attacks; confirm and manage identities and ultimately, reduce IP theft, fraud and cyber crime.**

|  |
| --- |
| **What have we been doing and what have we been investing in over the past 2 decades?**  **SALES**  **We are working on hiring sales function in Boston, New York, Nashville, Houston, Chicago, Reston, Santa Clara, San Francisco, and Seattle**  **ENGINEERING**  **We will need to hire Java Developers, QA engineers, Platform Infrastructure Engineer, Development Operations Engineers**  **PROFESSIONAL SERVICES**  **We will need to hire Security Product Implementation Consultants, Technical Support Engineers, Principal GRC Analysts**  **MARKETING**  **Product Marketing Managers, Public Relations Specialists, Technical Marketing Managers, Senior Consultants, Marketing Operations Specialists, Field Marketing Business Partners** |

Has your company learned the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work? Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

Is JED Consulting the right consultant for you?

STOP and ask yourself the following questions:

1. Do you fully understand why some organizations get compromised and others do not?
2. If there were compromised systems on your network, are you confident that you would be able to find them?
3. Do you know the effectiveness of each security device and are you certain that they are all configured correctly?
4. Are proper security metrics set up and communicated to your executives to drive security decisions?

If you do not know the answers to these questions, JED will provide the information security training and guidance you need to address these issues based on more than two decades of research and development.

The JED Consulting Services mission has taken aim at the major cybersecurity threats organizations face as they balance the security, compliance, and innovation required to thrive in this quickly changing market.

One case study is that healthcare organizations are increasingly under attack, and it's time for security practitioners to shore up their defenses! Through the latest research efforts, in-depth technical knowledge and vendor solutions, our customers will develop cyber hygiene strategies that address the most pressing issues in healthcare today: ransomware, data breaches, security awareness training, and understanding their health eco-system and where ePHI resides.

###### Topics and discussions will include:

* The true state of Cybersecurity in Healthcare and how critical cybersecurity has become for healthcare.
* How the CIS Critical Security Controls, promote cyber-hygiene in healthcare and defend healthcare organizations from the onslaught of attacks.
* World-renowned incident response handlers explain how they detected and responded to large healthcare breaches.
* New ransomware and other threat vectors; and how vendors are updating their solutions
* Determining the significance of a security incident
* The impact of a mature security awareness program

Our organization will bring together information security professionals working for hospital groups, health insurers, pharmaceutical companies, medical device manufacturers, and other healthcare related organizations to address key issues for:

* Chief Information Security Officers (CISO)
* Cyber security professionals
* Incident Responders
* Security architects
* Security risk managers
* Compliance professionals

The targeting and theft of sensitive health information continues to challenge covered entities and business associates alike. Increased regulation combined with a dynamic threat landscape require today's health care leader to have a clear understanding of relevant legislation and how to measurably defend patient data and related systems.

Our Health Care Security group is designed to provide your organization with an introduction to current and emerging issues in health care information security and regulatory compliance. The goal is to provide a foundational set of skills and knowledge for through the integration of case studies, hands-on labs, and defensible control considerations for securing and monitoring electronic protected health information ("ePHI"). The objective is to learn about actual attacks and incidents that have affected health care organizations and what can be done to mitigate the damage to prevent your organization from suffering a similar outcome. For compliance and audit professionals, this engagement will detail how to automate controls in support of the Health Insurance Portability and Accountability Act ("HIPAA") Security Rule and other key regulations.

**Why Choose JED Consulting Services LLC?**

* The HIPAA Security Rule provides the "what" in regard to requirements with which health care organizations must comply, yet we're often asked "how can we implement safeguards that fulfill the intent of the rule?" and "what else should HCO's be doing to protect patient and hospital assets?". This company is purposefully built to provide an effective answer.
* Our Health Care Security Group dissects the Security Rule and highlights important security controls to identify and mitigate both the insider and external based attacks.

If you are an information security professional working in health care, our company will provide you with practical advice for stopping even the most advanced attacks that may target the organization.

**Overview**

Our initial focus was on existing threats to health care information systems and data. We will examine 'why' and 'how' patient information is being targeted, as well as evolving trends, including, but not limited to the commercialization of malicious software, medical identity theft, and insider threats. JED also provides clients with an overview of the HIPAA Security Rule and its context, with close attention paid to the rules structure, safeguards, and the implementation specifications governing ePHI. This information will remove ambiguity and get of how to defend patient data and other sensitive information. The section concludes with a discussion on security frameworks, controls, and practical countermeasures.

Who in your organization has done an analysis of recent breach data? Who has focused on sensitive asset identification and hardening? Do we have a foundation for a data loss prevention ("DLP") program?

JED Consulting Services begins with examining the risk analysis requirement of the Security Rule, §164.308(a)(1)(ii)(A) along with relevant audit findings and important considerations for developing a defensible risk management process. Physical and technical safeguards are also examined. Have we then transition to a review of electronic health records ("EHR") security, often a prized target by criminals, and EHR application assessment and hardening? JED Health Care Security group concludes by discussing the current state of medical device security and risk management processes.

Hands-on exercises covered include log monitoring and analysis techniques, vulnerability assessment, asset encryption, and configuration analysis. Additional labs may be added, time permitting.

**What can we do to Implement and audit the critical controls we have focused on since 1989?**

* Apply a security framework based on actual threats that is measurable, scalable, and reliable in stop- ping known attacks and protecting organizations' important information and systems
* Understand the importance of each control, how it is compromised if ignored, and explain the defensive goals that result in quick wins and increased visibility of network and systems
* Identify and utilize tools that implement controls through automation
* Learn how to create a scoring tool for measuring the effectiveness of each controls the effectiveness of each control
* Employ specific metrics to establish a baseline and measure the effectiveness of security controls
* Understand how critical controls map to standards such as NIST 800-53, ISO 27002, the Australian Top 35, and more
* Audit each of the critical security controls, with specific, proven templates, checklists, and scripts provided to facilitate the audit process

We will cover an introduction and overview of the Critical Security Controls, laying the foundation for the rest of the engagement. For each control the following information will be covered, and we will follow the same outline for each control:

1. Overview of the Control
2. How it is Compromised
3. Defensive Goals
4. Quick Wins
5. Visibility & Attribution
6. Configuration & Hygiene
7. Advanced
8. Overview of Evaluating the Control
9. Core Evaluation Test(s)
10. Testing/Reporting Metrics
11. Steps for Root Cause Analysis of Failures
12. Audit/Evaluation Methodologies
13. Evaluation Tools
14. Exercise to Illustrate Implementation Or Steps for Auditing a Control

* **Critical Control 1:** Inventory of Authorized and Unauthorized Devices
  + Any time a new device is installed on a network, the risks of exposing the network to unknown vulnerabilities or hampering its operation are present.
  + Malicious code can take advantage of new hardware that is not configured and patched with appropriate security updates at the time of installation.
  + Attackers can use these vulnerable systems to install backdoors before they are hardened. In automating critical control 1, it is critical for all devices to have an accurate and up-to-date inventory control system in place.
  + Any device not in the database should be prohibited from connecting to the network.
  + Some organizations maintain asset inventories by using specific large-scale enterprise commercial products or by using free solutions to track and sweep the network periodically.
  + To evaluate the implementation of Control 1 on a periodic basis, the evaluation team will connect hardened test systems to at least 10 locations on the network.
  + This will include a selection of subnets associated with DMZs, workstations, and servers.
* **Critical Control 2:** Inventory of Authorized and Unauthorized Software
  + An organization without the ability to inventory and control its computers' installed programs makes its systems more vulnerable to attack.
  + Furthermore, poorly controlled machines are more likely to be running software that is unneeded for business purposes, introducing potential security flaws.
  + Compromised systems become a staging point for attackers to collect sensitive information.
  + In order to combat this potential threat, an organization should scan a network and identify known or responding applications.
  + Commercial software and asset inventory tools are widely available.
  + The best tools provide an inventory check of hundreds of common applications, pulling information about the patch level of each installed program.
  + This ensures that it is the latest version and that it leverages standardized application names, like those found in the Common Platform Enumeration (CPE) specification.
  + In addition to inventory checks, tools that implement whitelists (allow) and blacklists (deny) of programs are included in many modern end-point security suites.
  + To evaluate the implementation of Control 2 on a periodic basis, the team must move a benign software test program that is not included in the authorized software list on 10 systems on the network.
  + The team must then verify that the software is blocked and unable to run.
* **Critical Control 3:** Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
  + Default configurations of software are often geared to ease-of-deployment and ease-of-use and not security, leaving some systems exploitable in their default state.
  + Attackers attempt to exploit both network-accessible services and client software using various forms of malware.
  + Without the ability to inventory and control installed and running, enterprises make their systems more vulnerable.
  + Organizations can implement this control by developing a series of images and secure storage servers for hosting these standard images.
  + Configuration management tools can be employed to measure the settings of the installed software and to look for deviations from the standard image configurations used by the organization.
  + To evaluate the implementation of Control 3 on a periodic basis, an evaluation team must move a benign test system (one that does not contain the official hardened image, but does contain additional services, ports, and configuration files changes) onto the network.
  + The evaluation team must then verify that the systems generate an alert or e-mail notice regarding the changes to the software.
* **Critical Control 4:** Continuous Vulnerability Assessment and Remediation
  + Soon after new vulnerabilities are discovered and reported by security researchers or vendors, attackers engineer exploit code and launch it against targets of interest.
  + Any significant delays finding or fixing software with critical vulnerabilities provides ample opportunity for persistent attackers to break through and gain control of vulnerable machines.
  + A large number of vulnerability scanning tools are available to evaluate the security configuration of systems.
  + The most effective vulnerability scanning tools compare the results of the current scan with previous scans to determine how the vulnerabilities in the environment have changed over time.
  + All machines identified by the asset inventory system must be scanned for vulnerabilities.
  + To evaluate the implementation of Control 4 on a periodic basis, the evaluation team must verify that scanning tools have successfully completed their weekly or daily scans.
* **Critical Control 5:** Controlled Use of Administrative Privileges
  + The most common method attackers use to infiltrate a target enterprise is through an employee's own misuse of administrator privileges.
  + An attacker can easily convince a workstation user to open a malicious e-mail attachment, download and open a file from a malicious site, or surf to a site that automatically downloads malicious content.
  + If the user is logged in as an administrator, the attacker has full access to the system.
  + Built-in operating system features can extract lists of accounts with super-user privileges, both locally on individual systems and on overall domain controllers.
  + These accounts should be monitored and tracked very closely.
  + To evaluate the implementation of Control 5 on a periodic basis, an evaluation team must verify that the organization's password policy is enforced and administrator accounts are carefully controlled.
  + The evaluation team does this by creating a temporary, disabled, limited privilege test account on ten different systems.
  + It then attempts to change the password on the account to a value that does not meet the organization's password policy.
* **Critical Control 6:** Maintenance, Monitoring, and Analysis of Audit Logs
  + At times, audit logs provide the only evidence of a successful attack.
  + Many organizations keep audit records for compliance purposes but rarely review them.
  + When audit logs are not reviewed, organizations do not know their systems have been compromised. Attackers rely on this.
  + Most free and commercial operating systems, network services, and firewall technologies offer logging capabilities.
  + Such logging should be activated, and logs should be sent to centralized logging servers.
  + The system must be capable of logging all events across the network.
  + The logging must be validated across both network and host-based systems.
  + To evaluate the implementation of Control 6 on a periodic basis, an evaluation team must review the security logs of various network devices, servers, and hosts.
* **Critical Control 7:** Email and Web Browser Protections
  + Web browsers and email clients are very common points of entry and attack because of their high technical complexity and flexibility, and their direct interaction with users and within the other systems and websites.
  + Content can be crafted to entice of spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks.
  + Organizations must minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.
* **Critical Control 8:** Malware Defenses
  + Malicious software is an integral and dangerous aspect of Internet threats.
  + It targets end users and organizations via Web browsing, e-mail attachments, mobile devices, and other vectors.
  + Malicious code may tamper with a system's contents, capture sensitive data, and spread to other systems.
  + To ensure anti-virus signatures are up-to-date, effective organizations use automation.
  + They use the built-in administrative features of enterprise endpoint security suites to verify that anti-virus, anti-spyware, and host-based Intrusion Detection Systems (IDS) features are active on every managed system.
  + They also run automated assessments daily and review the results to find and mitigate systems that have deactivated such protections or do not have the latest malware definitions.
  + The system must identify any malicious software that is either installed, attempted to be installed, executed, or attempted to be executed, on a computer system.
  + To evaluate the implementation of Control 8 on a periodic basis, the evaluation team must move a benign software test program appearing to be malware onto a system and make sure it is properly discovered and remediated.
* **Critical Control 9:** Limitation and Control of Network Ports, Protocols, and Services
  + Attackers search for remotely accessible network services that are vulnerable to exploitation.
  + Many software packages automatically install services and turn them on as part of the installation of the main software package.
  + When this occurs, the software rarely informs a user that the services have been enabled.
  + Port scanning tools are used to determine which services are listening on the network for a range of target systems.
  + In addition to determining which ports are open, effective port scanners can be configured to identify the version of the protocol and service listening on each discovered open port.
  + The system must be capable of identifying any new unauthorized listening network ports that are connected to the network.
  + To evaluate the implementation of Control 9 on a periodic basis, the evaluation team must install hardened test services with network listeners on ten locations on the network, including a selection of subnets associated with DMZs, workstations, and servers.
* **Critical Control 10:** Data Recovery Capability (validated manually)
  + When attackers compromise machines, they often make significant changes to configurations and software.
  + Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information.
  + Once per quarter, a testing team should evaluate a random sample of system backups by attempting to restore them on a test bed environment.
  + The restored systems should be verified to ensure that the operating system, application, and datum from the backup are all intact and functional.
* **Critical Control 11:** Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
  + Attackers penetrate defenses by searching for electronic holes in firewalls, routers, and switches.
  + Once these network devices have been exploited, attackers can gain access to target networks, redirect traffic on that network (to a malicious system masquerading as a trusted system), and intercept and alter information while in transmission.
  + Organizations can use commercial tools that will evaluate the rule set of network filtering devices, which determine whether they are consistent or in conflict and provide an automated check of network filters.
  + Additionally, these commercial tools search for errors in rule sets. Such tools should be run each time significant changes are made to firewall rule sets, router ACLs, or other filtering technologies.
  + To evaluate the implementation of Control 11 on a periodic basis, an evaluation team must make a change to each type of network device plugged into the network.
  + At a minimum, routers, switches, and firewalls need to be tested. If they exist, IPS, IDS, and other network devices must be included.
* **Critical Control 12:** Boundary Defense
  + By attacking Internet-facing systems, attackers can create a relay point to break into other networks or internal systems.
  + Automated tools can be used to exploit vulnerable entry points into a network.
  + To control the flow of traffic through network borders and to look for attacks and evidence of compromised machines, boundary defenses should be multi-layered
  + These boundaries should consist of firewalls, proxies, DMZ perimeter networks, and network-based intrusion prevention systems and intrusion detection systems.
  + Organizations should regularly test these sensors by launching vulnerability-scanning tools.
  + These tools verify that the scanner traffic triggers an appropriate alert.
  + The captured packets of the Intrusion Detection Systems (IDS) sensors should be reviewed using an automated script each day, which ensures log volumes are within expected parameters, are formatted properly, and have not been corrupted.
  + To evaluate the implementation of Control 12 on a periodic basis, an evaluation team must test boundary devices.
  + This is done by sending packets from outside a trusted network, which ensures that only authorized packets are allowed through the boundary.
  + All other packets must be dropped.
* **Critical Control 13:** Data Protection
  + The loss of protected and sensitive data is a serious threat to business operations, and potentially, national security.
  + While some data is leaked or lost as a result of theft or espionage, the vast majority of these problems result from poorly understood data practices.
  + These include, but are not limited to, a lack of effective policy architectures and user error.
  + The phrase "Data Loss Prevention" (DLP) refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework.
  + Commercial DLP solutions are available to look for exfiltration attempts and detect other suspicious activities associated with a protected network holding sensitive information.
  + The system must be capable of identifying unauthorized datum leaving the organization's systems whether via network file transfers or removable media.
  + To evaluate the implementation of Control 13 on a periodic basis, the evaluation team must attempt to move test datum sets (that trigger DLP systems but do not contain sensitive data) outside of the trusted computing environment via both network file transfers and via removable media
* **Critical Control 14:** Controlled Access Based On Need to Know
  + Some organizations do not carefully identify and separate sensitive data from less sensitive, publicly available information within an internal network.
  + In many environments, internal users have access to all or most of the information on the network.
  + Once attackers have penetrated such a network, they can easily find and exfiltrate important information with little resistance.
  + This control is often implemented using the built-in separation of administrator accounts from non-administrator accounts.
  + The system must be able to detect all attempts by users to access files without the appropriate privileges and must generate an alert or e-mail for administrative personnel.
  + This includes information on local systems or network accessible file shares. To evaluate the implementation of Control 14 on a periodic basis, the evaluation team must create test accounts with limited access and verify that the account is unable to access controlled information.
* **Critical Control 15:** Wireless Device Control
  + Attackers who gain wireless access to an organization from nearby parking lots have initiated major data thefts.
  + This allows attackers to bypass an organization to maintain long-term access inside a target.
  + Effective organizations run commercial wireless scanning, detection, and discovery tools as well as commercial wireless intrusion detection systems.
  + The system must be capable of identifying unauthorized wireless devices or configurations when they are within range of the organization's systems or connected to its networks.
  + To evaluate the implementation of Control 15 on a periodic basis, the evaluation team staff must configure unauthorized but hardened wireless clients and wireless access points to the organization's network.
  + It must also attempt to connect them to the organization's wireless networks. These access points must be detected and remediated in a timely manner.
* **Critical Control 16:** Account Monitoring and Control
  + Attackers frequently impersonate legitimate users through inactive user accounts.
  + This method makes it difficult for network watchers to identify attackers' behavior.
  + Although most operating systems include capabilities for logging information about account usage, these features are sometimes disabled by default.
  + Security personnel can configure systems to record more detailed information about account access and utilize homegrown scripts or third-party log analysis tools to analyze this information.
  + The system must be capable of identifying unauthorized user accounts when they exist on the system.
  + To evaluate the implementation of Control 16 on a periodic basis, the evaluation team must verify that the list of locked out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire has successfully been completed daily.
* **Critical Control 17:** Security Skills Assessment and Appropriate Training to Fill Gaps (validated manually)
  + An organization hoping to find and respond to attacks effectively relies on its employees and contractors to find the gaps and fill them.
  + A solid security skills assessment program can provide actionable information to decision makers about where security awareness needs to be improved.
  + It can also help determine proper allocation of limited resources to improve security practices.
  + The key to upgrading skills is measurement, not with certification examinations, but with assessments that show both the employee and the employer where knowledge is sufficient and where there are gaps.
  + Once the gaps have been identified, those employees who have the requisite knowledge can be called upon to mentor the employees who do not.
  + The organization can also develop training programs that directly maintain employee readiness
* **Critical Control 18:** Application Software Security
  + Criminal organizations frequently attack vulnerabilities in both web-based and non-web-based application software.
  + In fact, it is a top priority for criminals. Application software is vulnerable to remote compromise in three ways:
    - It does not properly check the size of user input
    - It fails to sanitize user input by filtering out potentially malicious character sequences
    - It does not initialize and clear variables properly
  + To avoid attacks, internally developed and third party application software must be carefully tested to find security flaws.
  + Source code testing tools, web application security scanning tools, and object code testing tools have proven useful in securing application software.
  + Another useful tool is manual application security penetration testing by testers who have extensive programming knowledge and application penetration testing expertise.
  + The system must be capable of detecting and blocking an application-level software attack, and must generate an alert or send e-mail to enterprise administrative personnel.
  + To evaluate the implementation of Control 18 on a monthly basis, an evaluation team must use a web application vulnerability scanner to test software security flaws.
* **Critical Control 19:** Incident Response and Management (validated manually)
  + Without an incident response plan, an organization may not discover an attack in the first place.
  + Even if the attack is detected, the organization may not follow proper procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion.
  + Thus, the attacker may have far higher impact on the target organization, causing more damage, infecting more systems, and possibly exfiltrating more sensitive data than would otherwise be possible.
  + After defining detailed incident response procedures, the incident response team should engage in periodic scenario-based training.
  + This includes, but is not limited to, working through a series of attack scenarios that are fine-tuned to the threats and vulnerabilities the organization faces.
* **Critical Control 20:** Penetration Tests and Red Team Exercises (validated manually)
  + Attackers penetrate networks and systems through social engineering and by exploiting vulnerable software and hardware.
  + Penetration testing involves mimicking the actions of computer attackers, and exploiting them to determine what kind of access an attacker can gain. Each organization should define a clear scope and the rules of engagement for penetration testing and red team analyses.
  + The scope of such projects should include, at least, systems with the highest value information and production processing functionality.

What can JED Do about Incident Handling?

* Apply incident handling processes-including preparation, identification, containment, eradication, and recovery-to protect enterprise environments
* Analyze the structure of common attack techniques in order to evaluate an attacker's spread through a system and network, anticipating and thwarting further attacker activity
* Utilize tools and evidence to determine the kind of malware used in an attack, including rootkits, backdoors, and Trojan horses, choosing appropriate defenses and response tactics for each
* Use built-in command-line tools such as Windows tasklist, wmic, and reg, as well as Linux netstat, ps, and lsof to detect an attacker's presence on a machine
* Analyze router and system ARP tables along with switch CAM tables to track an attacker's activity through a network and identify a suspect
* Use memory dumps and memory analysis tools to determine an attacker's activities on a machine, the malware installed, and other machines the attacker used as pivot points across the network
* Gain access to a target machine using Metasploit, and then detecting the artifacts and impact of exploitation through process, file, memory, and log analysis
* Analyze a system to see how attackers use the malware to move files, create backdoors, and build relays through a target environment
* Run the Nmap port scanner and Nessus vulnerability scanner to find openings on target systems, and apply tools such as tcpdump and netstat to detect and analyze the impact of the scanning activity
* Apply the tcpdump sniffer to analyze network traffic generated by a covert backdoor to determine an attacker's tactics
* Employ the netstat and Isof tools to diagnose specific types of traffic-flooding denial-of-service techniques, and choose appropriate response actions based on each attacker's flood technique
* Analyze shell history files to find compromised machines, attacker-controlled accounts, sniffers, and backdoors

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose doesn't!), your computer systems will get attacked?

From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

* By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, this course helps you turn the tables on computer attackers. It addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still prevalent, and everything in between.
  + Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them.
  + In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.
  + Finally, students will participate in a hands-on workshop that focuses on scanning for, exploiting, and defending systems. It will enable you to discover the holes in your system before the bad guys do!
* Who in your organization is well-suited to lead or are a part of an incident handling team. General security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

**Overview**

Securing an infrastructure is a complex task of balancing business needs against security risks. With the discovery of new vulnerabilities almost on a daily basis, there is always the potential for an intrusion. In addition to online intrusions, physical incidents like fires, floods, and crime all require a solid methodology for incident handling to be in place to get systems and services back online as quickly and securely as possible.

The first part of this section looks at the invaluable Incident Handling Step-by-Step model, which was created through a consensus process involving experienced incident handlers from corporations, government agencies, and educational institutes, and has been proven effective in hundreds of organizations. This section is designed to provide students a complete introduction to the incident handling process, using the six steps (preparation, identification, containment, eradication, recovery, and lessons learned) one needs to follow to prepare for and deal with a computer incident.

The second part of this section examines from-the-trenches case studies to understand what does and does not work in identifying computer attackers. This section provides valuable information on the steps a systems administrator can take to improve the chances of catching and prosecuting attackers.

**Topics**

Preparation

* Building an incident response kit
* Identifying your core incident response team
* Instrumentation of the site and system

Identification

* Signs of an incident
* First steps
* Chain of custody
* Detecting and reacting to Insider Threats

Containment

* Documentation strategies: video and audio
* Containment and quarantine
* Pull the network cable, switch and site
* Identifying and isolating the trust model

Eradication

* Evaluating whether a backup is compromised
* Total rebuild of the Operating System
* Moving to a new architecture

Recovery

* Who makes the determination to return to production?
* Monitoring to system
* Expect an increase in attacks

Special Actions for Responding to Different Types of Incidents

* Espionage
* Inappropriate use

Incident Record-keeping

* Pre-built forms
* Legal acceptability

Incident Follow-up

* Lessons learned meeting
* Changes in process for the future

**Overview**

Seemingly innocuous data leaking from your network could provide the clue needed by an attacker to blow your systems wide open. Who in your organization understands details associated with reconnaissance and scanning, the first two phases of many computer attacks.?

Your networks reveal an enormous amount of information to potential attackers. In addition to looking for information leakage, attackers also conduct detailed scans of systems, scouring for openings to get through your defenses. To break into your network, they scope out targets of opportunity, such as weak DMZ systems and firewalls, unsecured modems, or the increasingly popular wireless LAN attacks. Attackers are increasingly employing inverse scanning, blind scans, and bounce scans to obscure their source and intentions. They are also targeting firewalls, attempting to understand and manipulate rule sets to penetrate our networks. Another very hot area in computer attacks involves Intrusion Detection System evasion, techniques that allow an attacker to avoid detection by these computer burglar alarms.

If you do not have the skills needed to understand these critical phases of an attack in detail, you will not be able to protect your network. Does your organization understand these attacks and the associated defenses?

It is imperative that you get written permission from the proper authority in your organization before using these tools and techniques on your organization's systems. You also need to advise your network and computer operations teams of your testing schedule.

**Exercises**

Hands-on Exercises with the Following Tools:

* InSSIDer for Wireless LAN discovery
* Nmap Port Scanner and Operating System fingerprinting tool
* Nessus Vulnerability Scanner
* Windows Command Line Kung-Fu for extracting Windows data through SMB sessions

**Topics**

Reconnaissance

* What does your network reveal?
* Are you leaking too much information?
* Using Whois lookups, ARIN, RIPE and APNIC
* Domain Name System harvesting
* Data gathering from job postings, websites, and government databases
* Recon-ng
* Pushpin
* Identifying publicly compromised accounts
* Maltego
* FOCA for metadata analysis

Scanning

* Locating and attacking unsecure wireless LANs
* War dialing with War-VOX for renegade modems and unsecure phones
* Port scanning: Traditional, stealth, and blind scanning
* Active and passive Operating System fingerprinting
* Determining firewall filtering rules
* Vulnerability scanning using Nessus and other tools
* CGI scanning with Nikto
* Powershell Empire
* Bloodhound
* Rubber Duckie attacks to steal wireless profiles
* User Behavioral Analytics

Intrusion Detection System (IDS) Evasion

* Foiling IDS at the network level
* Foiling IDS at the application level: Exploiting the rich syntax of computer languages
* Web Attack IDS evasion tactics
* Bypassing IDS/IPS with TCP obfuscation techniques

Computer attackers are ripping our networks and systems apart in novel ways, while constantly improving their techniques. The third step of many hacker attacks is: gaining access.

Attackers employ a variety of strategies to take over systems from the network level up to the application level. This section covers the attacks in depth, from the details of buffer overflow and format string attack techniques to the latest in session hijacking of supposedly secure protocols. Who in your organization has hands-on experience in running sniffers and the incredibly flexible Netcat tool?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Administrators need to get into the nitty-gritty of how the attacks and their associated defenses work if they want to effectively defend against these invasions. For each attack, the course explains the vulnerability, how various tools exploit it, the signature of the attack, and how to harden the system or application against the attack. Students who sign an ethics and release form are issued a DVD containing the attack tools examined in class.

It is imperative that you get written permission from the proper authority in your organization before using these tools and techniques on your organization's system. You also need to advise your network and computer operations teams of your testing schedule.

**Exercises**

Hands-on Exercises with the Following Tools:

* Sniffers, including Tcpdump
* Sniffer detection tools, including ifconfig, ifstatus, and promiscdetect
* Netcat for transferring files, creating backdoors, and setting up relays
* Metasploit, Metasploit, Metasploit Lots of Metasploit
* ARP and MAC analysis for ARP cache poisoning attack detection

**Topics**

Network-Level Attacks

* Session hijacking: From Telnet to SSL and SSH
* Monkey-in-the-middle attacks
* Passive sniffing

Gathering and Parsing Packets

* Active sniffing: ARP cache poisoning and DNS injection
* Bettercap
* Responder
* LLMNR poisoning
* WPAD Attacks
* MITMf
* DNS cache poisoning: Redirecting traffic on the Internet
* Using and abusing Netcat, including backdoors and nasty relays
* IP address spoofing variations

Operating System and Application-level Attacks

* Buffer overflows in-depth
* The Metasploit exploitation framework
* Format string attacks
* AV and application whitelisting bypass techniques

Netcat: The Attacker's Best Friend

* Transferring files, creating backdoors, and shoveling shell
* Netcat relays to obscure the source of an attack
* Replay attacks

**Overview**

One of the attackers' favorite techniques for compromising a network , is a worm. We will analyze worm developments over the last two years and project these trends into the future to get a feel for the coming Super Worms we will face. Then the issue turns to another vital area often exploited by attackers: web applications. Because most organizations' homegrown web applications do not get the security scrutiny of commercial software, attackers exploit these targets using SQL injection, cross-site scripting, session cloning, and a variety of other mechanisms discussed in detail.

The engagement also presents a taxonomy of nasty denial-of-service attacks, illustrating how attackers can stop services or exhaust resources, as well as what you need to do to prevent their nefarious deeds.

Once intruders have gained access into a system, they want to keep that access, preventing pesky system administrators and security personnel from detecting their presence. To fool you, attackers install backdoor tools and manipulate existing software on a system to maintain access to the machine on their own terms. To defend against these attacks, you need to understand how attackers alter systems to discover the sometimes-subtle hints associated with system compromise. This engagement arms you with the understanding and tools you need to defend against attackers' maintaining access and covering their tracks.

It is imperative that you get written permission from the proper authority in your organization before using these tools and techniques on your organization's system. You also need to advise your network and computer operations teams of your testing schedule.

**Exercises**

Hands-on Exercises with the Following Tools and Topics:

* Password cracking
* Cross-site scripting and SQL injection web application attacks
* Detecting DoS attacks

**Topics**

Password Cracking

* Analysis of worm trends
* Password cracking with John the Ripper
* Hashcat
* Rainbow Tables
* Password spraying

Web Application Attacks

* Account harvesting
* SQL Injection: Manipulating back-end databases
* Session Cloning: Grabbing other users' web sessions
* Cross-Site Scripting

Denial-of-Service Attacks

* Distributed Denial of Service: Pulsing zombies and reflected attacks
* Local Denial of Service

**Overview**

The fourth and fifth steps of many hacker attacks: maintaining access and covering their tracks. Computer attackers install backdoors, apply Rootkits, and sometimes even manipulate the underlying kernel itself to hide their nefarious deeds. Each of these categories of tools requires specialized defenses to protect the underlying system. We will analyze the most commonly used malicious code specimens, as well as explore future trends in malware, including BIOS-level and combo malware possibilities.

Attackers also cover their tracks by hiding files, sniffers, network usage, and active processes. Additionally, super stealthy sniffing backdoors are increasingly being used to thwart investigations. Finally, attackers often alter system logs, all in an attempt to make the compromised system appear normal. Does your organization have the tools and techniques you need to detect and respond to these activities on your computers and network?

It is imperative that you get written permission from the proper authority in your organization before using these tools and techniques on your organization's system. You also need to advise your network and computer operations teams of your testing schedule.

**Exercises**

Hands-on Exercises with the Following Tools:

* RootKits and detection
* Detecting backdoors with Netstat, lsof
* Hidden file detection with LADS
* Covert channels using Covert\_TCP
* HTTP Reverse Shells using Base64

**Topics**

Maintaining Access

* Backdoors: Using Poison Ivy, VNC, Ghost RAT, and other popular beasts
* Trojan horse backdoors: A nasty combo
* Rootkits: Substituting binary executables with nasty variations
* Kernel-level Rootkits: Attacking the heart of the Operating System (Rooty, Avatar, and Alureon)

Covering the Tracks

* File and directory camouflage and hiding
* Log file editing on Windows and Unix
* Accounting entry editing: UTMP, WTMP, shell histories, etc.
* Covert channels over HTTP, ICMP, TCP, and other protocols
* Sniffing backdoors and how they can really mess up your investigations unless you are aware of them
* Steganography: Hiding data in images, music, binaries, or any other file type
* Memory analysis of an attack

**Putting It All Together**

* Specific scenarios showing how attackers use a variety of tools together
* Analyzing scenarios based on real-world attacks
* Learning from the mistakes of other organizations
* Where to go for the latest attack info and trends
* Over the years, the security industry has become smarter and more effective in stopping hackers. Unfortunately, hacker tools are becoming smarter and more complex. One of the most effective methods to stop the enemy is to actually test the environment with the same tools and tactics an attacker might use against you.
* This workshop lets you put what you have learned over the past week into practice. You will be connected to one of the most hostile networks on earth. This network simulates the Internet and allows students to try actual attacks against live machines and learn how to protect against these attacks. This workshop will supplement the classroom training that students have already received and give them flight time with the attack tools to better understand how they work. Instructors will give guidance on exactly what is happening as exploits and defensive measures are running. As students work on various exploits and master them, the environment will become increasingly difficult, so students will have to master additional skills in order to successfully complete the exercises.
* Additionally, students can participate in the workshop's Capture the Flag event. By penetrating systems, discovering subtle flaws, and using puzzle-solving techniques, you can test the skills you have built over the week in this engaging contest. The Capture the Flag victors will win a prize.
* In sum, paranoia is good! Your laptop will be attacked. Do not have any sensitive data stored on the system. JED is not responsible for your system if (actually, when) someone in the class attacks it in the workshop. Bring the right equipment and prepare it in advance to maximize what you will learn and the fun you will have doing it.

## Drive security transformation without introducing new risk

Building the right security strategy that accelerates new IT trends, addresses skills shortages, and staying ahead of rapidly changing techniques is critical to a creating a more proactive and mature security environment.

IBM® Security can help you design an integrated framework with security management solutions, systems integration and managed services to protect the enterprise.

# 2016 Cyber Security Intelligence Index

### Serious data breaches, major attacks and new vulnerabilities

#### Understand the threat landscape to improve your security posture

There’s very little that cyber criminals can do today that’s truly new—and yet, 2015 was filled with serious incidents across the entire industry.

The annual IBM® X-Force® Cyber Security Intelligence Index report offers a high-level overview and detailed look at the type and volume of attacks, which industries are most affected, and the key factors enabling attackers to help you better understand the current threat landscape. It reveals how security threats are evolving year to year, and provides well-informed insights about the impact they can have on your organization.

Based on operational data collected from thousands of devices monitored in over 100 countries, the 2016 Cyber Security Intelligence Index from IBM Security Services was created by the IBM X-Force research team, which works diligently to keep clients informed and prepared for the latest cybersecurity threats.

## Welcome to the new era of cognitive security

At IBM® Security, we’re training a new generation of systems to understand, reason and learn about constantly evolving security threats. We’re beginning to build security instincts and expertise into new defenses that analyze research reports, web text and threat data – just like security professionals do every day – but with unprecedented speed and scale.

Enter cognitive security. Built upon security intelligence, cognitive solutions generate not just answers, but hypotheses, evidence-based reasoning and recommendations for improved decision making in real time. As a result, cognitive security will help address the current skills gap, accelerate responses and help reduce the cost and complexity of dealing with cybercrime.

For almost a century, we’ve programmed computers to help solve complex problems. We can now simulate weather, sequence genomes and instantly share data across the world. But ask a computer to do something humans do every day—recognize an image, read a book or explain the meaning of a poem—and it’s a different story. Traditional systems fall short.

The same is true for security. For decades, we’ve programmed computers to recognize viruses, malware and exploits. We continuously tune them to become more accurate, but it’s not enough. Adversaries constantly morph their attacks and find creative ways to breach defenses. What organizations need is the ability to detect the subtlest change in activity and analyze it with as much context as possible to distinguish and eliminate new threats.

**80% of the world's data is unstructured**

It takes constant monitoring and maximum use of data to find attacks and abnormal behavior before damage is done. But the world produces over 2.5 quintillion bytes of data every day, and 80% of it is unstructured. This means it’s expressed in natural language – spoken, written or visual – that a human can easily understand but traditional security systems can’t. The reality is that there are thousands of security blogs posted every day with detailed threat intelligence. But it’s impossible for a security analyst to know everything that’s in them, and traditional security is unable to analyze and apply this insight the way an analyst can. This is why the most challenging security problems still require people to make sound decisions about what to act on and what’s a false alarm. In fact, the best security professionals build their body of knowledge every day through experience, talking with colleagues, attending conferences and staying up-to-date on research.

At IBM Security, we’re training a new generation of systems to understand, reason and learn about constantly evolving security threats. We’re beginning to build security instincts and expertise into new defenses that analyze research reports, web text, threat data and other security-relevant structured and unstructured data – just like security professionals do every day – but at a scale like we’ve never seen. This is the essence of cognitive security.

The result: analysts will call upon cognitive systems to help augment and even automate their understanding of a threat... making analysts smarter about the latest attacks and freeing up valuable time to focus on other pressing issues.

What is cognitive security?

Cognitive systems are self-learning systems that use data mining, machine learning, natural language processing and human–computer interaction to mimic the way the human brain works.

Cognitive security is the implementation of two broad and related capabilities:

•The use of cognitive systems to analyze security trends and distill enormous volumes of structured and unstructured data into information, and then into actionable knowledge to enable continuous security and business improvement

•The use of automated, data-driven security technologies, techniques and processes that support cognitive systems’ having the highest level of context and accuracy

From compliant to cognitive

Since the age of the first networks and the hackers who soon followed, we’ve evolved security technology to stop attacks. To date, there have been two distinct eras of cyber security: perimeter controls and security intelligence. These serve as building blocks as we enter the third era—cognitive security.

Perimeter controls: security that confines (pre-2005)

We started with static defenses to guard or limit the flow of data, including firewalls, antivirus software and web gateways. The evolution of information security within the enterprise began as a compliance exercise.

The goal was to lock down and restrict access to sensitive information via passwords and a range of access control strategies. Success meant passing an audit. While perimeter defenses are still in use, they are not sufficient by themselves for today’s environment.

**Security intelligence: security that helps you think (2005+)**

Over time, we progressed to sophisticated monitoring systems that can collect and comb through massive amounts of data to discover vulnerabilities and prioritize potential attacks. This transition led to a focus on real-time information to detect suspicious activity. Today, security intelligence is the real-time collection, normalization and analysis of structured data, generated by users, applications and infrastructure.

**Cognitive security: security that understands, reasons and learns at scale (2015+)**

Security intelligence uses analytics to detect deviations from regular patterns, uncover changes in network traffic and find activities that exceed defined levels. Within a security intelligence infrastructure, analytics are applied to massive amounts of information in an effort to understand company data within context and prioritize day-to-day activities. By determining which deviations are meaningful, security intelligence can not only help detect compromises faster, but also reduce false positives to save time and resources.

Built upon security intelligence, which leverages big data analytics, cognitive security is characterized by technology that is able to understand, reason and learn. A much greater scale of relevant security data is now accessible with cognitive systems that can process and interpret the 80% of today's data that's unstructured, such as written and spoken language.

After ingesting a corpus of knowledge, curated by experts on any given subject, a cognitive security system is trained by being fed a series of question-and-answer pairs. This machine “knowledge” is then enhanced as security professionals interact with the system, providing feedback on the accuracy of the system’s responses. A key difference: a cognitive system comprehends and processes new information at a speed that far surpasses any human. Technical defenses can now be trained to analyze thousands of research reports, conference materials, academic papers, news articles, blog posts and industry alerts—every day.

As cognitive systems continue to observe events and behaviors—distinguishing the good from the bad—the ability to leverage integrated defenses to block new threats gets stronger and stronger. By helping to make security analysts more effective and accelerating the response to emerging threats, cognitive security will help to address the current security skills gap, bringing heightened levels of confidence and risk control. Se

Illustration showing the progression of security from perimeter controls to security intelligence to cognitive security during the more than ten year period from pre-2005 to 2015

Cognitive ultimately plays into a framework built on the basics of traditional security. Security intelligence is not going away; it’s a key building block of cognitive security. What cognitive does is gives us a way to triage threat intelligence and detection, and provide actionable information, at a speed and scale like never before.

Illustration of the additional level of understanding that cognitive brings to traditional security intelligence and big data analytics

Because security intelligence and big data analytics are traditionally unstructured, the cognitive element brings an important additional level of understanding to what’s going on and how to act. With this full stack, you can have the maximum amount of protection available for your security environment. See figure 2.

The cognitive security edge

Traditional, programmable security systems respond to requests, make determinations and analyze data according to predefined parameters. Cognitive systems interpret data, add to their base of knowledge from virtually every interaction, weigh probabilities based on a depth of insight and help you take action based on consideration of relevant variables.

Whereas the current generation of systems are reactive—detecting and responding to anomalies or attacks—cognitive security is proactive. Forward focused and continuously multi-tasking, cognitive systems scour for vulnerabilities, connect dots, detect variances and sift through billions of events to build upon a base of actionable knowledge.

Cognitive solutions generate not just answers, but hypotheses, evidence-based reasoning and recommendations. What’s possible now is the ability to interpret the 80 percent of data that’s unstructured - previously inaccessible to existing systems – and integrate it with structured data from countless sources and locations. In a global economy where value increasingly comes from information, data represents one of the most abundant, valuable and complex raw materials in the world. We now have the means to mine both structured and unstructured data, and continuously extract features and patterns to provide context in real time for improved decision making.

The following three pillars of cognitive security function in a rapid-fire pace of human-like thought patterns:

1. Understand and make sense of unstructured data and natural language text. This includes the ability to ingest and process information through “reading” books, reports, blogs and relevant industry data, “seeing” images and “hearing” natural speech within its context.

2. Reason based on the ability to interpret and organize information and offer explanations of what it means, along with a rationale for conclusions.

3. Learn continuously as data accumulates and insights are derived from interaction.

**Digging deeper, going wider**

A single-minded focus on detecting malware, malicious threats, outliers and anomalies can tend to result in too many false positives. That’s the advantage of the multidimensional playing field in which cognitive systems operate.

In today’s world, the ability to distinguish among black and white is just one aspect of the expertise required for an integrated security infrastructure. There’s an increasing amount of grey area, and that’s where cognitive comes in.

Fortified with heightened levels of intuition, intelligence and insight, cognitive systems are designed to be continuously enhanced with data to help distinguish acceptable behaviors from subtle variations that could signal emerging threats. The result is a broader perspective and a proactive focus on the big picture.

**Addressing the skills gap**

It’s not just our systems that are challenged in keeping up with today’s security environment; there are challenges on the staff side as well. The number of unfilled information security positions around the world is estimated at 208,000 and is expected to grow to 1.5 million by 2020. Cognitive security can help.

Serving as a scalable resource to support human capabilities, cognitive systems can act like extraordinary extensions to often understaffed security departments. This new dimension is vital because it’s no longer enough to keep a close watch on what’s happening within your own system. You need to monitor threats on a global scale in order to prepare for potential attacks. Cognitive systems are able to tap into global exchange networks that analyze hundreds of thousands of security events per second, for thousands of clients around the world.

Cognitive can ease the task of the security analyst by providing human-centric communications, such as advanced visualizations, interactive vulnerability analysis, risk assessment, remediation and possible attribution. Cognitive systems will be able to spot anomalies and flawed logic, and provide evidence-based reasoning. This enables analysts to weigh alternative outcomes and improve decision making.

Use cases: cognitive unleashed

#1 Enhance your SOC analysts

Cognitive systems can understand a vast sea of structured and unstructured data, to help quickly move the value of a junior analyst from a level 1 to a 2 or 3. Cognitive systems can automate ingesting information – such as research reports and best practices – to give real-time input. Previously, this knowledge and insight could only be obtained from years of experience.

#2 Speed your response with external intelligence

When the next malware hits, people will blog about how to protect your organization from it. Even though a signature is not available yet, there is natural language online that can help you answer the question. Cognitive systems can crawl to quickly discover how to protect against the next zero-day exploit.

#3 Identify threats with advanced analytics

Cognitive systems may use analysis methods such as machine learning, clustering, graph mining and entity relationship modeling to identify potential threats. They can help speed detection of risky user behavior, data exfiltration and malware detection before damage occurs.

#4 Strengthen Application Security

Cognitive systems can understand the semantic context of your analytics and data, while exploring code and code structures. They can take thousands of vulnerability findings and refine results to a small set of actionable items – and take you to locations in your code where you can fix them.

#5 Improve enterprise risk

In the future, cognitive systems could analyze corpuses of interactions, the nature of those interactions and their susceptibility to develop risk profiles for organizations, corporate actions, training and re-education. Cognitive systems could use natural language processing to find sensitive data in an organization and redact it.

The future: reversing cybercrime economics

Cognitive systems can analyze features, or characteristics, from an enormous set of malicious software—known as malware—in order to detect subtle commonalities. The reason why that’s key: the diversity of malicious software is huge, but cybercrime groups evolve their code, so much of the malware at work today is actually related to other malware. With cognitive systems, we can analyze thousands of features of a suspicious executable file and cluster them to uncover patterns. And without a human ever knowing what those features were, or how or why they matched, the system can identify a pattern that helps discover and classify new malware variants.

As the cognitive security community grows, and the viability of new attacks is diminished, cybercrime will enter into a new economic reality. Efforts to develop malware that evades detection will become increasingly complex and costly. According to the Ponemon Institute’s 2015 Cost of Data Breach Study, 256 days is the average time it takes organizations to detect advanced persistent threats; and $6.5 million is the average cost of a U.S. data breach. Cognitive security will empower security analysts with the capabilities to find early warnings of potential attacks and significantly speed detection. Cybercriminals will find the payoffs to be harder and harder to achieve.

Cognitive computing is driving transformational change by harnessing not just data, but meaning, knowledge, process flows and progression of activity at a lightning-fast speed and scope. For organizations that embrace cognitive capabilities, the competitive advantage will be significant and far-reaching.

Integration and expertise for a cognitive ecosystem

Integration and expertise are paramount to doing security right. Too many security practices are built on a collection of point products that are not integrated, and don’t provide the visibility and actionable intelligence you need to quickly respond.

It’s not complete integration until your domain capabilities can interact and communicate with one another across your hybrid IT environment, extending beyond your company walls across your entire ecosystem.

The right integration can help you get the visibility you need to respond swiftly to security incidents when they occur. Integration allows you to do more with less, which is a fundamental way to address the security skills gap.

New threats are discovered every day, which means security expertise and threat intelligence sharing are essential. If you don’t have top-grade expertise feeding into a set of solutions and cognition, you’re going to get behind quickly. IBM X-Force Exchange currently catalogs information on more than 88,000 vulnerabilities, more than 25 billion web pages and data from 100 million endpoints—enabling real-time and global coverage of expertise that’s immediately actionable.

How JED can help

The cognitive journey is just beginning, but JED has the intellectual and financial strength to lead this revolution within security. JED is partnering with more than 7,500 IBM Security professionals, in 36 security centers worldwide, monitor 133 countries and 35 billion events every day.

IBM’s investment in cognitive technologies spans decades and has seen great progression in the last five years—the ability to process natural language, the ability to process voice and images, and the ability to turn unstructured data into tools like knowledge graphs that are easily analyzed. IBM will embrace cognitive, to continually enhance security use cases and bring that information back to security analysts.

IBM Security has cognitive capabilities available in solutions today. Machine learning is used to help increase the detection accuracy of vulnerabilities, and prioritize those vulnerabilities so you can respond much faster. Behavioral learning is used to proactively anticipate and find anomalies around threats that are happening in the network.

IBM Security offers end-to-end protection and an immune system approach that spans deep analytics, identity and access, advanced fraud, data, application, network, endpoint, cloud, mobile and research. Each of these platforms is going to benefit from IBM’s cognitive capabilities. If you’re interested in the benefits of cognitive security, think about adopting IBM’s platforms, which will be innovated and infused with cognitive technologies.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world’s broadest security research, development and delivery organizations, monitors 35 billion security events per day in 133 countries, and holds more than 3,700 security patents.

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We’ll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit ibm.com/financing

Why Work With a CISSP?

## Why JED Consulting has worked with SANS and ISACA?

## Training + Consulting = Solutions to Real Problems

Organizations need solutions that ensure employees have the proper skills and give them ways to fix their problems.

JED goal is to be the premier consulting organization and uses SANS for all of their customers training needs. The founder of JED also attends SANS and ISACA on a regular basis. More information and upcoming conferences can be found at [www.sans.org](http://www.sans.org/) or www.isaca.org,

SANS is the most trusted and by far the largest source for information security and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system – Internet Storm Center.

The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A range of individuals from auditors and network administrators, to chief information security officers are sharing the lessons they learn and are jointly finding solutions to the challenges they face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community.

A key foundational course that we recommend is SEC401 Security Essentials. Security Essentials teaches you all of the core components you need to be effective in network security. For calendar of dates and to register for a course, please visit [www.sans.org](http://www.sans.org/).

The following are some comments from students who have taken the course:

* "I have learned more in one week than in the past 2 years"  
  **Fernando R., Navy**
* "The best instructor/presentation I ever had – very energetic, very live, and very interesting. KEEP IT UP!!"  
  **Anonymous**
* "It's amazing how much information is clarified daily on subjects that I use "in theory" everyday at my job."  
  **Brenda Cattell, High County Bank**
* "Before this course, I had a false sense of security. Thank you for opening my eyes."  
  **Sang Paik, County of Orange, Health Care Agency**
* "This should be mandatory for anyone responsible for IS Security/Auditing. The tools and identified threats will help those to gain the knowledge necessary to become experts for their company/agency."  
  **Michael Klatt, Raytheon**
* "Your classes are extremely informational and thorough. You set a great pace, are upbeat and add good entertainment to keep our attention focused. Great job, keep it up!"  
  **Javier Streb, Cornell University**
* "I strongly believe I received what I came for and more. This was a great class indeed!"  
  **Javier Streb, Cornell University**

Who are the key Players and issues in this the Security Space?

Build Trust and Resilience at the Speed of Business

Peter Firstbrook, Vice President, Gartner Research;

Felix Gaehtgens, Director, Gartner Research;

Jeffrey Wheatman, Director, Gartner Research

Tom Scholtz, Vice President and Gartner Fellow, Gartner Research, and Conference Chair

|  |
| --- |
| JED has expertise to help your organization develop and enhance:  Chief Information Security Officer (CISO) Program  IT Security Program Tech Insights:  Security Architecture  Risk Management and Compliance Program Business Continuity Management (BCM) Program  The Marketplace for Security Program Workshops |

Top 100 Issues and who you are going to call about ?

1. State of Security Governance 2016 Jeffrey Wheatman
2. Roadmap Convergence: The State of IoT and OT Security 2016 Earl Perkins
3. State of Cloud Security 2016 Jay Heiser
4. An Attacker’s View on Malware Protection Technologies Mario de Boer
5. Propel Your Business With Innovation Risk Management John A. Wheeler
6. The Gartner Risk Treatment Model: Fixing Accountability and Risk Sign-Off Paul E. Proctor
7. State of Business Resilience 2016 Roberta J. Witty
8. State of the Security Markets Sid Deshpande
9. Creating Differentiated Value Michele C. Caminos
10. We Analyze Too Much and Synthesize Too Little Frank Buytendijk
11. Understanding Why Bimodal IT Demands More Agile Security Jeremy D’Hoinne, Paul E. Proctor
12. The Mobile Security Scenario John Girard
13. Protecting Workloads in Hybrid Cloud-Data Center Architectures Neil MacDonald
14. Case Study: Security and Compliance for Time Inc.’s Move to the Cloud (AWS) Keith O’Sullivan, VP/CISO Global Information Security, Time Inc.
15. Designing Security Into the Internet of Things: A Technical Primer Ramon Krikken
16. Gartner Essentials: Results of the 2016 Security and Risk Surveys Khushbu Pratap
17. Women in IT: Business Transformation Requires Workplace Diversity Debra Logan, Roberta J. Witty
18. Responding to Business Interruptions: A Proven Methodology to Minimize Event Impacts Ken Otis
19. The Future of Sales for Security Providers Perry Carpenter, Sid Deshpande
20. Developing, Implementing and Optimizing Security-Monitoring Use Cases Augusto Barros, Anton Chuvakin
21. Security 2020 — The Future of Cybersecurity Rob McMillan
22. State of the Threat Environment 2016 Greg Young
23. How Digital Business Reshapes Mobile Security Dionisio Zumerle
24. State of Application Security 2016 Ramon Krikken
25. Understanding and Implementing Security in Office 365: Exchange, SharePoint and OneDrive Patrick Hevesi
26. Eliminating the Risk Buried in Your Unstructured Dark Data Alan Dayley
27. Case Study: An Unconventional Approach to Develop Real Recovery Goals Brad Krueger, CISSP, CISA, Business Resiliency Senior Manager, CMFG Life Insurance Company
28. The Impact of Cloud Security Requirements on Security Market Segments Sid Deshpande
29. Bimodal IT and Security Governance — Friend or Foe? Rob McMillan, Tom Scholtz
30. Detecting Insider Threats and Abuse Avivah Litan
31. 2016 Enterprise DLP Magic Quadrant Review Brian Reed
32. Design Principles for User-Friendly Mobile Security John Girard
33. Security for Mobile Apps Using SDKs, Wrapping and Hardening Ramon Krikken
34. The NIST Risk Management Framework— What Agencies Need to Know Katell Thielemann
35. Magic Quadrant for IT Vendor Risk Management Christopher Ambrose
36. Govern for Success: How to Establish BCM Program Governance Belinda Wilson
37. IoT Security — Market Opportunity or Hype? Ruggero Contu
38. Women in IT Reception Avivah Litan, Debra Logan, Roberta J. Witty, Jie Zhang
39. CISO Circle Power Breakfast: A Smart City Gets Innovative With Cyber Gary Hayslip, CISO, City of San Diego; F. Christian Byrnes
40. The New Threat Landscape in Healthcare Greg Barnes, CISO, Horizon Blue Cross Blue Shield of New Jersey; Haddon Bennett, CISO, Change Healthcare; Mark Burnette, Partner, LBMC Information Security; Mark Johnson, Managing Director, KPMG LLP; Ray Wagner
41. Security Governance Trends and Leading Practices in the Public Sector Bob Smock
42. Understanding ITSecurity Program Maturity in Higher Education Kevin K. Kampman, Steven L. Kaplan
43. Digital Ethics — When Saying ‘I’m Sorry’ Is Not Enough Frank Buytendijk, Vice President and Gartner Fellow, Gartner Research
44. Identity and Access Management In the Digital Business Ant Allan
45. State of Data Security 2016 Brian Reed
46. Information-Centric Mobile Security: Your Data Can Move Without Leaking John Girard
47. Hybrid SIEM: Using Service Providers to Improve Security Kelly M. Kavanagh
48. IT Risk Assessment and Measurement: Common Traps and Practical Approaches Erik T. Heidt
49. Governing Risk and Security in the Digital Business Tom Scholtz
50. Cybersecurity and Risk Management in Digital Business Paul E. Proctor
51. Developing Contingency Plans for Your Most Critical Vendors Christopher Ambrose
52. How Threat Intelligence Sharing Will Transform the Future Security Market Lawrence Pingree
53. How to Build Your Security Strategy Rob McMillan
54. Experiences From Implementing Mobile Identity Rob Smith
55. Top Security Predictions/SPAs 2016 John A. Wheeler
56. Protecting Your Website Against DDoS and Other Threats Jeremy D’Hoinne, Lawrence Orans
57. The Technology and Deployment Options Behind a CASB Craig Lawson, Neil MacDonald
58. Information 2020 — Cracking Critical Dilemmas Frank Buytendijk
59. How to Run A SIEM Operation Anton Chuvakin
60. Identifying, Monitoring and Mitigating Critical Vendor Risks Christopher Ambrose
61. Case Study: Damon Stokes, Senior Manager of Governance, Risk and Performance, Blue Cross Blue Shield of Michigan; Jie Zhang
62. Panel: Crisis and Incident Management Andrew Marinik, Emergency Planner, Emergency Management, Virginia Polytechnic Institute and State University; Roberta J. Witty
63. How to Use Technology to Support People-Centric Security Perry Carpenter, Tom Scholtz
64. Taking Charge General Colin Powell, USA (Ret.)
65. Digital Humanism and Security: How PeopleCentric Security Will Help Paul E. Proctor, Tom Scholtz
66. The Future of Network Security Cool Vendors and New Technologies in Security 2016 Neil MacDonald
67. Why the Internet of Things Will Make All of Us Physical Security Professionals Earl Perkin
68. Toward a Data-Centric Security Architecture Mario de Boer
69. How to Keep Your Legal Counsel and Compliance Officer Happy When Migrating to Office 365 Alan Dayley, Jie Zhang
70. Critical Capabilities for Operational Risk Management Solutions John A. Wheeler
71. The Value Stream Approach to BCM Lori Norman, MBCI, CPP, Director, Organizational Resilience, WEX; Roberta J. Witty
72. Firewall Market: Buying Behaviors and Budget Trends for 2016 Lawrence Pingree
73. Get Incident-Ready — Test Your Plan With a Scenario Rob McMillan, Andrew Walls
74. Self-Assessing Your Organization’s Mobile Security John Girard, Dionisio Zumerle
75. How to Outsource Security Functions Effectively Sid Deshpande
76. Who’s First in theRecovery Queue? William Delaney, Belinda Wilson
77. Combating Cybercrime in the Financial Services Industry Tom Scholtz
78. The Future of Technology and Geopolitics Dr. Peter Singer, Strategist, New America Foundation
79. Beyond the Impossible Lewis Pugh, Ocean Advocate, Maritime Lawyer and Leading Inspirational Speaker
80. Socio-Analyzing IT Control: Leveraging Social Science to Improve IT Control Tom Scholtz
81. Top Cybersecurity Trends for 2016-2017 Earl Perkins
82. Roadmap/State of Endpoint Security Eric Ouellet
83. Security Monitoring Options for SMBs Toby Bussa
84. The World Is Changing: How Does It Affect My Vulnerability Management Program? Augusto Barros
85. Panel: Globalization of Personal Data Stops Here —Did Europe Pull the Brake? Carsten Casper Maverick
86. The Unbearable Cost of Privacy Brian Iverson
87. Women in IT: How to Conduct a Self-Evaluation So You Don’t Sell Yourself Short Deb Wheatman, President, Careers Done Write
88. Crossfire: Brainstorming and Debating the Next Evolution of IAM Ant Allan, Perry Carpenter,Felix Gaehtgens, Brian Iverson, Avivah Litan, David Anthony Mahdi, Anmol Singh, Ray Wagner
89. The Languages of Change: Overcoming Change Resistance Debra Logan, Christie Struckman
90. Navigating the Political Layer —Tactics to Protect and Grow Your Security Budget Rob McMillan
91. The Three Things You Need to Do to Benefit From Threat Intelligence Craig Lawson
92. Magic Quadrant and Critical Capabilities — Enterprise Mobility Management Suites Rob Smith
93. Enterprise Network Firewalls Magic Quadrant Adam Hils
94. Insider Threat Insights Form Recent Research Erik T. Heidt
95. Implementing the Cybersecurity Framework and the Risk Management Framework Paul E. Proctor, Katell Thielemann
96. The Art of Leading a HighPerformance BCM Team Debra Logan
97. Navigating the Chaotic World of Security Analytics Eric Ahlm, Avivah Litan
98. Digital Humanism and the CISO Richard Hunter
99. The New CISO’s Crucial First 100 DaysTom Scholtz
100. State of Security Monitoring and Analytics 2016 Toby Bussa, Avivah Litan
101. Stop Data Breaches — Protect the Data! Brian Lowans
102. Keeping SaaS Secure Jay Heiser
103. How to Build Your Next-Generation Mobile Security Strategy Patrick Hevesi
104. Panel: Globalization of Personal Data Stops Here — Did Europe Pull the Break? Peter Blenkinsop, Partner, Drinker Biddle; Carsten Casper
105. Case Study: Where’s the Digital BEEF? The BC Paradox — Unlocking Better BC Data, Plans and Resilience Joe Woulfe, Vice President of Business Continuity Management, Rabobank
106. Case Study: Big Data, Cloud Computing, the Perfect Trade Control Storm? Or Opportunity?David Harris, Global IT Trade Control Focal, Intellectual Property Focal, Boeing
107. Report Cybersecurity and IT Risk to Your Board of Directors Paul E. Proctor
108. The Five Tests You Must Apply to Your Security Metrics Rob McMillan, Jeffrey Wheatman
109. Case Study: : Integrating Security in DevOps — DevSecOps Neil MacDonald
110. Where Identity and Data Security Meet David Anthony Mahdi
111. Controlling Applications With Malware Protection and the User in Mind Mario de Boer
112. What Are Customer Expectations for Privacy? Jenny Sussin
113. How to Build Advanced KRIs — Risk Metrics That Influence Business Decisions Paul E. Proctor
114. Women in IT: How to Conduct a Self-Evaluation So You Don’t Sell Yourself Short Debra Wheatman, President, Careers Done Write; Roberta J. Witty
115. Who Are You Selling To? Being Intentional With Role-Specific Messaging to Get Your Buyer’s Attention Michele C. Caminos, Perry Carpenter
116. Using the ‘Predict, Prevent, Detect, Respond’ Framework to Communicate Your Security Program Strategy Perry Carpenter : Monetization of Data Security Will Bring Balanced Investment Decisions Brian Lowans
117. Get Me a Secure Line!Protecting Communications With Voice and Texting Encryption Dionisio Zumerle
118. The Intelligence-Driven SOC Oliver Rochford
119. Cloud Computing Security Strategies Erik T. Heidt
120. What Federal Agencies Need to Know About Software Asset Management Victoria Barber, Katell Thielemann
121. One Simple Way to Get Your CEO to Embrace Risk Management John A. Wheeler
122. What Every Security Vendor Should Know About Security Automation Eric Ahlm
123. Doing Business Securely in China Jie Zhang.
124. Embracing Cybersecurity in Higher Education Steven L. Kaplan, Heidi Schmidt Katell Thielemann
125. The Risks of Digital Business Richard Hunter,
126. Overcoming Security Staffing Challenges to Embrace Digital Business Jeremy D’Hoinne
127. State of IAM 2016 Felix Gaehtgens
128. Gentrifying the Neglected Network Security in Public and Private Clouds Greg Young
129. Next-Generation Endpoint Protection Peter Firstbrook
130. Demystifying Security Analytics: Data, Methods and Use Cases Anton Chuvakin
131. Effective SOD Controls: A Risk-Based Approach to Segregation of Duties in Enterprise Applications Anmol Singh
132. Digital Risk Officer Paul E. Proctor J13.
133. Essential Communication and Conflict Resolution Skills for Security Leaders Perry Carpenter
134. Communicating to the Media During a Crisis Ann Baldwin, President, Baldwin Media Marketing; Roberta J. Witt
135. Three Easy Steps to a Down-and Dirty Risk Register Jeffrey Wheatman
136. How to Avoid Having a Really Bad Day — Preparing for and Managing Security Incidents in a Controlled Way Rob McMillan
137. Dealing With Your Encrypted Traffic Visibility Problems Adam Hils
138. Absolute Identity Proofing Is Dead; Use Dynamic Identity Assessment Instead Avivah Litan
139. MSSP or In-House. Battle of Security Outsourcing Anton Chuvakin, Augusto Barros
140. Managing Software Asset Risks in Outsourced and Cloud Environments — Tools and Techniques Victoria Barber
141. Shifting Delivery Models in Security — Cloud-Based Security Ruggero Contu
142. Securing the Digital Supply Chain of Your Organization Earl Perkins
143. Rocks and Sand — Doing the Simple Things Well Has Never Been More ImportantCraig Lawson
144. How to be Secure in Amazon Web Services Steve Riley
145. Best Practices in DDoS Defenses —Understand the Options Available Claudio

**Security Market Descriptions**

# Application Security

A majority of today’s traditional attacks utilize application security weaknesses rather than those found in the applications supporting devices or operating systems. This is a result of two things; first, effective network security controls are better understood and implemented; and second, properly securing applications requires a significantly higher level of effort when compared to security networks.

JED Security understands our clients’ desires to not only discover and remediate application specific vulnerabilities, but also integrate security into their software development life-cycles (SDLC).

JED Security’s Application Security services include:

* Application Architecture Assessment
* Application Penetration Testing
* Application Vulnerability Scanning
* Application Vulnerability Assessment
* Database Security Assessment
* Secure Code Review
* Secure Software Development Life-cycle (SDLC) Development

# Incident Response and Forensics

In a recent study, more than seventy percent of businesses reported suffering a security breach of some kind within their organization. Evidence suggests that this figure will only continue to rise. With today’s threat landscape ever-increasing, organizations must realize that it is only a matter of time before they suffer a material breach. Organizations that accept this realization are better prepared to appropriately respond to a material incident and understand the importance of their response. Those who refuse to accept this realization risk significant operating and financial penalties resulting from inappropriate or improper reporting and responses.

JED Security enables our clients to better prevent material incidents by identifying and limiting the exposure of confirmed attacks. Having our clients understand their capabilities as well as their roles and responsibilities during an incident better enables them to make the right decisions, including when to utilize our services.

JED Security’s Incident Response and Forensics services include:

* Digital Forensics
* Incident Detection and Containment
* Incident Response Plan Development and Review
* Incident Response Retainer Services
* Malware Analysis / Reverse Engineering
* Network Threat Analysis
* Table Top Exercises

# Security Assessments

The need for Security Assessments such as vulnerability assessment and penetration testing is clearly understood by information security practitioners. Most information security services organizations offer some form of Security Assessment services, however as most industry professionals will agree, not all assessors are created equal. Every experienced information security professional has horror stories from past Security Assessment experiences.

JED Security’s professionals are some of the industry’s most experienced and professional practitioners. Their experience is derived from both a consulting and corporate security background, and are considered thought leaders throughout the industry. Our clients trust JED Security’s professionals to perform Security Assessments against even the most delicate of infrastructure such as SCADA and SmartGrid environments. This trust is earned by our professionals with each and every Security Assessment engagement and is core value of JED Security.

JED Security’s Security Assessment services include:

* Penetration Testing
* Secure Configuration Review
* Social Engineering Testing
* Vulnerability Assessment
* Vulnerability Scanning
* War Dialing
* Wireless Security Assessment

**Your Mission Is Our Goal**

As you know, before you can concentrate on the growth of business, it's important to secure your critical intellectual property (IP). This is the mission of JED. We focus on the entire IP life cycle, from identification to protection. Everything we do is focused on giving you a competitive advantage.

What distinguishes JED from other security entities is our ability to address unique security needs with creative solutions. Because every customer is different, every solution we provide is customized.

Key advantages to working with JED:

* We partner with you to achieve your goals
* We deliver distinctive solutions — no cookie-cutter approach
* We focus on solutions, not just problems
* All JED consultants are highly educated, ethical and experienced and prepared to fulfill the entire spectrum of your needs. We follow the Code of Ethics of the ISC2 , Institute of Internal Auditors ,ISACA, and AICPA. We have a MBA from Rensselaer (RPI), we have attended classes at MIT, and graduated from Northeastern University after making a significant impact on the university.

## Key Offerings

**Assessment** - If you lack the resources to address security issues, consider an independent assessment. It will pinpoint high-risk areas and provide creative recommendations to secure your environment.

**Penetration Test** - This is an advanced simulation of attackers trying to find ways into your organization. While most of our competitors only focus on success or failure, we team with you to provide high-end testing that identifies a full list of vulnerabilities.

**Threat Analysis** - In order to defend your network you need to appreciate how hackers work and operate. JED specializes in understanding the techniques, tools and mindset of attackers. This allows us to provide real-world solutions that help you focus on critical areas. JED also identifies new threats by running honeypots, including wireless, IPv6 and IPv4.

**Intellectual Property Analysis** - To protect your intellectual property, you need to identify what it is. JED has worked with organizations and venture capital firms to identify critical intellectual property and areas that could be patented. We also help companies understand whether data would be best protected with a trade secret or patent. If either is desired, we can organize and facilitate the process. We have worked one CTO with over 98 United States Patents.

**Network Design and Security** - JED specializes in the total network integration process. We assist organizations like yours in building networks from the ground up, filled with robust security and functionally.

**Product Analysis** - Some organizations are already aware of their key threats and vulnerabilities and simply need assistance in deciding what solutions to implement. JED has a deep understanding of the solutions process across a wide range of offerings. By performing a thorough requirements analysis, we can make solid recommendations that match your security profile.

**Writing and Presenting** – JED has partnered with consultants who are experts in their respective fields and are constantly writing and presenting on key topics. As master presenters, we can help you promote your products and provide better visibility into new markets.

**Technical Market Analysis** - JED provides consulting services to help better position products and make additional sales. We offer keen insight as to what new clients in emerging markets may need, with sensitivity towards the investment they are willing to make.

**Compliance Analysis** - With new regulations constantly being passed it is critically important that companies stay aware and compliant. JED has unique solutions for helping organizations achieve compliance with mandates such as PCI, SOX, GLBA and HIPAA.

**General Consulting** - Occasionally, customers are not certain what their needs are or where to begin. Our consultants are highly skilled and work with you to help identify high-risk items and the best course of action. JED provides services based on hourly, weekly or monthly rates, including retainer agreements.

**Publications & Resources**

Our mission is not only to provide customized solutions for your security needs. We also strive to provide informational resources to keep you educated and up to date with security trends. The following articles, white papers and corporate newsletters are available for download as helpful resources to assist you in navigating through the vast realm of information security and making informed decisions. We encourage you to investigate these topics and contact us with any questions you may have.

30 Things Every Manager Should Know

40 Top Security Tools

Security Best Practices

Security Newsletter Archive

Podcasts & Videos

As an industry expert, Dr. Eric Cole has teamed with Cisco Systems, Inc. for a series of informational presentations on current IT security issues and solutions, including a series on internal threats called "The Evil Insider." Contact John Donnelly to learn more about each program and then stream or download to learn what is new in the security industry.

Leveraging Security Intelligence

The Evil Insider vs. Network Admission Control

Securing Remote Access From the Evil Insider

Securing Customer Data From the Evil Insider

In addition to the above publications and podcasts, Dr. Eric Cole, CEO and Principal Security Consultant of Secure Anchor, is an active and popular author of books pertaining to IT security. Dr. Cole has authored and co-authored the following books:

Hackers Beware

Insider Threat

Cyber Spying

Network Security Bible

Hiding in Plain Sight

SANS GIAC Certification: Security Essentials Toolkit (GSEC)

Google the following links for more information.

Sans Institute

CVE - Common Vulnerabilities and Exposures

BlackHat

The Honeynet Project

IT Security

SecurityFocus

SC Magazine

ISACA

**What does John E. Donnelly III bring to the table?**

**Certified Information Systems Auditor** (**CISA**) is a globally recognized certification in the field of [audit](https://en.wikipedia.org/wiki/Audit), [control](https://en.wikipedia.org/wiki/Corporate_governance_of_information_technology) and [security](https://en.wikipedia.org/wiki/Information_security) of information systems. CISA gained worldwide acceptance having uniform certification criteria, the certification has a high degree of visibility and recognition in the fields of IT security, [IT audit](https://en.wikipedia.org/wiki/IT_audit), IT risk management and governance. Vacancies in the areas of IT security management, IT audit or IT risk management often ask for a CISA certification.[[1]](https://en.wikipedia.org/wiki/Certified_Information_Systems_Auditor#cite_note-1) The exam tends to be associated with a high failure rate. CISA is awarded by [ISACA](https://en.wikipedia.org/wiki/ISACA).[[](https://en.wikipedia.org/wiki/Certified_Information_Systems_Auditor#cite_note-2)

**Certified Information Systems Security Professional (CISSP) is an independent information security certification governed by the International Information System Security Certification Consortium, also known as (ISC)².**

**The CISSP curriculum covers subject matter in a variety of Information Security topics.[8] The CISSP examination is based on what (ISC)² terms the Common Body of Knowledge (or CBK). According to (ISC)², "the CISSP CBK is a taxonomy – a collection of topics relevant to information security professionals** around the world. The CISSP CBK establishes a common framework of information security terms and principles that allow information security professionals worldwide to discuss, debate and resolve matters pertaining to the profession with a common understanding."

From 2015, the CISSP curriculum is divided into eight domains:

Security and Risk Management

Asset Security

Security Engineering

Communications and Network Security

Identity and Access Management

Security Assessment and Testing

Security Operations

Software Development Security

Before 2015, it covered ten similar domains.



Certified Internal Auditor (CIA): Strengthen Your Core

The CIA journey begins with a focus on The IIA’s International Standards for the Professional Practice of Internal Auditing (Standards) and aspects of mandatory guidance under the IPPF. The journey continues with a focus on managing an internal audit project and culminates with concepts related to internal control, risk, governance, and technology. The CIA is a 3-part process for establishing your foundational core and starting point for career growth to:

* Distinguish you from your peers.
* Demonstrate your proficiency with internal staff and external clients.
* Develop your knowledge of best practices in the industry.
* Demonstrate your proficiency and professionalism.
* Lay a foundation for continued improvement and advancement

**Definition of Internal Auditing**

1. Define purpose, authority, and responsibility of the internal audit activity

**B. Code of Ethics**

1. Abide by and promote compliance with The IIA Code of Ethics

**C.  International Standards**

1. Comply with The IIA's Attribute Standards
   1. Determine if the purpose, authority, and responsibility of the internal audit activity are documented in audit charter, approved by the Board and communicated to the engagement clients
   2. Demonstrate an understanding of the purpose, authority, and responsibility of the internal audit activity
2. Maintain independence and objectivity
   1. Foster independence
      1. Understand organizational independence
      2. Recognize the importance of organizational independence
      3. Determine if the internal audit activity is properly aligned to achieve organizational independence
   2. Foster objectivity
      1. Establish policies to promote objectivity
      2. Assess individual objectivity
      3. Maintain individual objectivity
      4. Recognize and mitigate impairments to independence and objectivity
3. Determine if the required knowledge, skills, and competencies are available
   1. Understand the knowledge, skills, and competencies that an internal auditor needs to possess
   2. Identify the knowledge, skills, and competencies required to fulfill the responsibilities of the internal audit activity
4. Develop and/or procure necessary knowledge, skills and competencies collectively required by the internal audit activity
5. Exercise due professional care
6. Promote continuing professional development
   1. Develop and implement a plan for continuing professional development for internal audit staff
   2. Enhance individual competency through continuing professional development
7. Promote quality assurance and improvement of the internal audit activity
   1. Monitor the effectiveness of the quality assurance and improvement program
   2. Report the results of the quality assurance and improvement program to the board or other governing body
   3. Conduct quality assurance procedures and recommend improvements to the performance of the internal audit activity

**Internal Control / Risk (25-35%) – Awareness Level (A)**

**A. Types of Controls (e.g., preventive, detective, input, output, etc.)**

**B. Management Control Techniques**

**C. Internal Control Framework Characteristics and Use (e.g., COSO, Cadbury)**

1. Develop and implement an organization-wide risk and control framework

**D. Alternative Control Frameworks**

**E. Risk Vocabulary and Concepts**

**F. Fraud Risk Awareness**

1. Types of fraud
2. Fraud red flags

**III. Conducting Internal Audit Engagements – Audit Tools and Techniques (25-35%)**

**A. Data Gathering (Collect and analyze data on proposed engagements):**

1. Review previous audit reports and other relevant documentation as part of a preliminary survey of the engagement area
2. Develop checklists/internal control questionnaires as part of a preliminary survey of the engagement area
3. Conduct interviews as part of a preliminary survey of the engagement area
4. Use observation to gather data
5. Conduct engagement to assure identification of key risks and controls
6. Sampling  (non-statistical [judgmental] sampling method, statistical sampling, discovery sampling, and statistical analyses techniques)

**B. Data Analysis and Interpretation:**

1. Use computerized audit tools and techniques (e.g., data mining and extraction, continuous monitoring, automated work papers, embedded audit modules)
2. Conduct spreadsheet analysis
3. Use analytical review techniques (e.g., ratio estimation, variance analysis, budget vs. actual, trend analysis, other reasonableness tests)
4. Conduct benchmarking
5. Draw conclusions

**C. Data Reporting**

1. Report test results to auditor in charge
2. Develop preliminary conclusions regarding controls

**D. Documentation / Work Papers**

1. Develop work papers

**E. Process Mapping, Including Flowcharting**

**F. Evaluate Relevance, Sufficiency, and Competence of Evidence**

1. Identify potential sources of evidence

**I. Managing the Internal Audit Function (40-50%)**

**A. Strategic Role of Internal Audit**

1. Initiate, manage, be a change catalyst, and cope with change
2. Build and maintain networking with other organization executives and the audit committee
3. Organize and lead a team in mapping, analysis, and business process improvement
4. Assess and foster the ethical climate of the board and management
   1. Investigate and recommend resolution for ethics/compliance complaints, and determine disposition of ethics violations
   2. Maintain and administer business conduct policy (e.g., conflict of interest), and report on compliance
5. Educate senior management and the board on best practices in governance, risk management, control, and compliance
6. Communicate internal audit key performance indicators to senior management and the board on a regular basis
7. Coordinate IA efforts with external auditor, regulatory oversight bodies and other internal assurance functions
8. Assess the adequacy of the performance measurement system, achievement of corporate objective – Awareness Level (A)

**B.  Operational Role of IA**

1. Formulate policies and procedures for the planning, organizing, directing, and monitoring of internal audit operations
2. Review the role of the internal audit function within the risk management framework
3. Direct administrative activities (e.g., budgeting, human resources) of the internal audit department
4. Interview candidates for internal audit positions
5. Report on the effectiveness of corporate risk management processes to senior management and the board
6. Report on the effectiveness of the internal control and risk management frameworks
7. Maintain effective Quality Assurance Improvement Program

**C.  Establish Risk-Based IA Plan**

1. Use market, product, and industry knowledge to identify new internal audit engagement opportunities
2. Use a risk framework to identify sources of potential engagements (e.g., audit universe, audit cycle requirements, management requests, regulatory mandates)
3. Establish a framework for assessing risk
4. Rank and validate risk priorities to prioritize engagements in the audit plan
5. Identify internal audit resource requirements for annual IA plan
6. Communicate areas of significant risk and obtain approval from the board for the annual engagement plan
7. Types of engagements
   1. Conduct assurance engagements  
      a.1  Risk and control self-assessments  
              a) Facilitated approach  
                   (1)  Client-facilitated  
                   (2)  Audit-facilitated  
               b)  Questionnaire approach  
               c)  Self-certification approach  
        a.2  Audits of third parties and contract auditing  
        a.3  Quality audit engagements  
        a.4  Due diligence audit engagements  
        a.5  Security audit engagements  
        a.6  Privacy audit engagements  
        a.7  Performance audit engagements (key performance indicators)  
        a.8 Operational audit engagements (efficiency and effectiveness)  
        a.9  Financial audit engagements
   2. Compliance audit engagements
   3. Consulting engagements  
      c.1  Internal control training  
      c.2  Business process mapping  
      c.3  Benchmarking  
      c.4  System development reviews  
      c.5  Design of performance measurement systems

**II. Managing Individual Engagements (40-50%)**

**A.  Plan Engagements**

1. Establish engagement objectives/criteria and finalize the scope of the engagement
2. Plan engagement to assure identification of key risks and controls
3. Complete a detailed risk assessment of each audit area (prioritize or evaluate risk/control factors)
4. Determine engagement procedures and prepare engagement work program
5. Determine the level of staff and resources needed for the engagement
6. Construct audit staff schedule for effective use of time

**B. Supervise Engagement**

1. Direct / supervise individual engagements
2. Nurture instrumental relations, build bonds, and work with others toward shared goals
3. Coordinate work assignments among audit team members when serving as the auditor-in-charge of a project
4. Review work papers
5. Conduct exit conference
6. Complete performance appraisals of engagement staff

**C. Communicate Engagement Results**

1. Initiate preliminary communication with engagement clients
2. Communicate interim progress
3. Develop recommendations when appropriate
4. Prepare report or other communication
5. Approve engagement report
6. Determine distribution of the report
7. Obtain management response to the report
8. Report outcomes to appropriate parties

**D. Monitor Engagement Outcomes**

1. Identify appropriate method to monitor engagement outcomes
2. Monitor engagement outcomes and conduct appropriate follow-up by the internal audit activity
3. Conduct follow-up and report on management's response to internal audit recommendations
4. Report significant audit issues to senior management and the board periodically

**III. Fraud Risks and Controls (5-15%)**

**A. Consider the potential for fraud risks and identify common types of fraud associated with the engagement area during the engagement planning process**

**B.  Determine if fraud risks require special consideration when conducting an engagement**

**C.  Determine if any suspected fraud merits investigation**

**D. Complete a process review to improve controls to prevent fraud and recommend changes**

**E. Employ audit tests to detect fraud**

**F. Support a culture of fraud awareness, and encourage the reporting of improprieties**

**G.  Interrogation/investigative techniques**

**H. Forensic auditing**

|  |
| --- |
| *Running down a dream*  By Katherine Teitler  November 7, 2016 |
| Reading the daily security news, as many in the field do, I came across this quote on [InsuranceThoughtLeadership.com](http://insurancethoughtleadership.com/insurance-industry-can-solve-cyber/), written by Scott M. Kannry, CEO of Axio Global:  *“Anybody who knows anything about cyber is likely thinking, ‘It’s impossible to solve cyber risk!’ But what if we redefine ‘solve’ as: ‘to*provide security *leaders and firms with an accurate picture of their cyber exposure, with the ability to effectively manage the risk and with resiliency when an event happens.’”*  Though the quote and the article in its entirety were referring to how cyber risk insurance can help “solve” cyber, it occurred to me that this quote can—and possibly should—be applied to cybersecurity in general. |

**I felt so good, like anything was possible**

Cybersecurity is a lot like driving; towns and cities and their respective road crews can keep roads in ace condition and post all kinds of clearly marked signs for speed limits, road hazards, dangerous curves, blind driveways, and the like. Police can patrol the roads for dangerous or illegal driving. Car manufacturers can build cars with all types of safety features included. But at the end of the day, no matter how scrupulously manufacturers build vehicles, how highly regulated or enforced the laws, or how carefully drivers drive down the roads, accidents will happen. An animal could suddenly run into the road causing a driver to stop short and get rear ended. The car’s brakes could fail or a tire could go flat, forcing a collision. Excessive water on the road could result in the car hydroplaning into a ditch. Endless possibilities exist for monkey wrenches to appear in the system.

Just like security.

This is not new news to security practitioners; the industry knows (and lives) the mountains of obstacles which keep companies, data, and systems from impenetrability. Yet, despite knowing that no company is immune to a breach, the community hasn’t come around to the idea that managing security is actually managing shades of risk; security teams remain laser focused on the technical details for which they are responsible, failing to communicate to executive management, who want nothing more than to understand how security is helping the organization achieve business goals—i.e., reduce risk so the company can gain greater market share and generate more revenue. Executive management doesn’t expect security to be “perfect,” but security itself still considers any tree branch that falls into the road a “fail.”

**I hit cruise control and rubbed my eyes**

Nothing is absolute. In other words, as Kannry alluded to: “to effectively manage the risk with resiliency when an event happens,” security leaders first need to understand their cyber exposure and then translate that to risk—the language the business understands and uses, The take away here, though, is that most security departments today are still deficient in the ability to create a clear, actionable risk profile for their organizations.

The problem lies in how security practitioners refer to and think about security: in terms of “winning” or “losing.” Anything categorized as either a “win” or a “loss” is absolute. And security will never be absolute. The industry has already accepted the fact that at some point every organization will be breached, so why perpetuate the “winning *or* losing” myth? Wouldn’t it be more beneficial to measure security against progress made, without any arbitrary goal line as a demarcation point?

People like the idea of winning, though, so perhaps instead of completely upending the accepted nomenclature, “winning” could be redefined as “reducing risk” or “mitigating incidents in a shorter timeframe with fewer losses” rather than “no incident whatsoever.” Leadership expert Michael Santarcangelo calls this concept “an infinite game,” an excellent analogy and one that means the industry doesn’t have to do a 180° on its thinking.

**Workin’ on a mystery, goin’ wherever it leads**

They key isn’t solving anything, in the sense that “solve” connotes finality, and there is no end point in security (pun intended). Instead these shades of risk and making forward progress are the keys to effectively managing security programs and ensuring organizations remain resilient in the eventuality of an incident

**Data Analytics Training**

This three-day ACL Certified course is a comprehensive introduction to ACL™ Analytics, designed for new and beginner users who want to learn the concepts and features needed to start using ACL™ Analytics. In an interactive hands-on environment, you will learn fundamentals such as basic data concepts and how to work within the ACL™ Analytics environment, as well as integral skills such as how to conduct analysis steps and procedures and accomplish analysis objectives in ACL™ Analytics. You will learn the proper methodology and best practices for all five phases of the data analysis cycle (planning, importing, preparing, analyzing, and reporting). On the third day, basic scripting will be introduced. Through this comprehensive introduction and practical application, you will learn how to effectively use ACL™ Analytics to accomplish your audit and/or business objectives.

**Learning Objectives​**

Efficiently and effectively using ACL™ Analytics to achieve your analysis objectives, report your findings, and build a narrative of your organization’s data

Reduce time and resources needed to analyze data

Detect gaps and control failures

Leverage hundreds of built-in data analysis commands and tools

Access and reconcile data from various systems in order to identify potential issues

Identify outliers and issues

Analyze data to achieve objectives

Combine data from multiple source types in order to make comparisons between them

Identify trends between issues that may be indicative of the root cause(s) of the problem

Create working paper documentation detailing your objectives, the analysis steps taken to achieve them, and the results returned

Use basic scripting to automate processes and initiate continuous monitoring

Fields of Study: Auditing

Delivery-Method: This is a group-live, instructor-led course in an interactive classroom. This course introduces fundamental concepts and maintains a comprehensible, progressive approach that follows the five phases of the data analysis cycle. The course incorporates an instructor-led case study, which enhances the learning process by seeing how a typical audit/data analysis project is conducted in ACL™ Analytics.

Prerequisites: Minimal or no experience with ACL™ Analytics

Course Level: Basic