Sponsored by Tripwire

Reducing Risk Through Prevention: Implementing Critical Security Controls 1-4

June 2013

A SANS Whitepaper

Written by James Tarala

Introduction

In almost every year since 2000, the Internet Crime Complaint Center has reported an increase in cybersecurity crime reports by individuals and organizations. Over the last dozen years, the number of attacks reported in the United States seems to grow consistently over time with minor deviations, as seen in Figure 1.

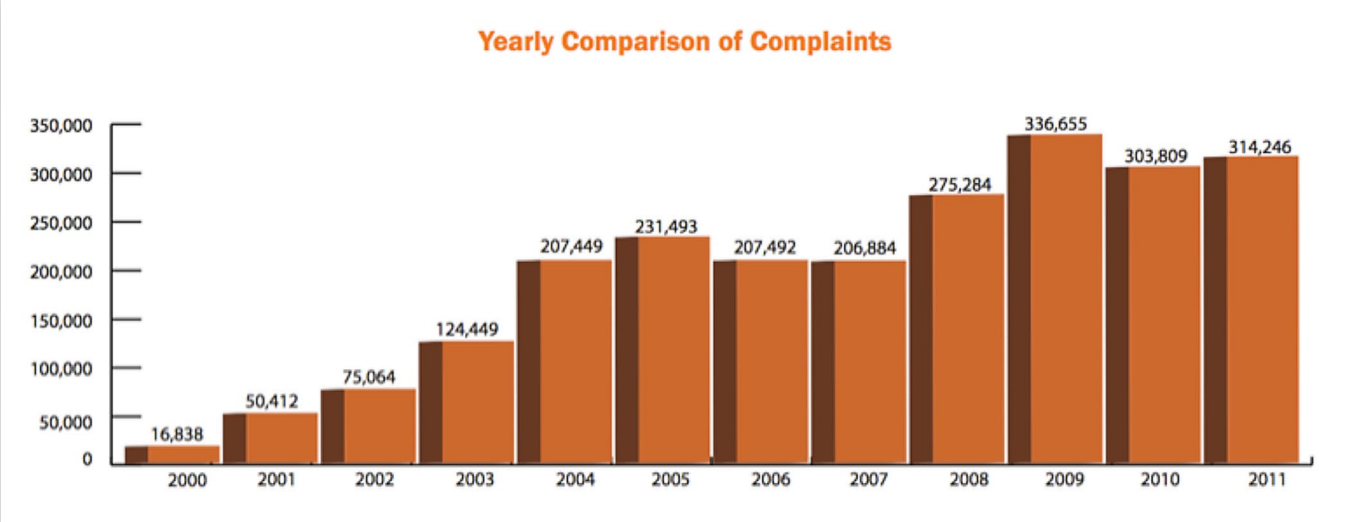

Figure 1. Internet-Related Complaints Reported to the FBI since 2000.[1]

After examining this trend, the question arises: Is there anything an organization can do to stop these attacks from occurring and protect their critical information systems from intruders?

Business leaders need to understand the risks that face their organization if they are to effectively mitigate those risks. In this SANS Analyst Program whitepaper, we will discuss the actual threats facing organizations today in a realistic and measured way. Then we will examine the methods dedicated attackers use to compromise systems using the "intrusion kill chain" as a model. Finally, we will consider specific defenses, as outlined by the first four Critical Security Controls (CSCs), which organizations can implement to keep future attacks from succeeding.

1 www.ic3.gov/media/annualreport/2011_IC3Report.pdf, p. 6

Cybersecurity Risks to Business Goals

Data breaches are happening every day, in every organization.

Hackers are unstoppable.

Even the most technologically savvy companies cannot stop hackers.

Business executives hear these frightening messages every day; the threat is real enough and too often realized. Verizon's 2013 Data Breach Investigations Report (DBIR) noted more than 47,000 reported security incidents, along with 621 confirmed data disclosures and at least 44 million compromised records in 2012 alone.[2] Yet with such a large portion of fear (and hype) being served without respite to executives, it becomes tough to know what is truly applicable to their organizations and how to implement suitable defenses. Paralysis or inaction may be the most likely responses to such reports, because how can an ordinary executive know the appropriate response?

As with any discussion of risk, an organization needs to understand what may be at stake should an Internet-based attack on vulnerable data or systems succeed. For instance:

- Would the organization lose sales to competitors?
- Would distributors refuse to distribute product?
- Would employees and union members walk off the job or refuse to produce goods or services?
- Could employees or other personnel be physically harmed?
- Would the organization's quarterly or annual filings be impacted?
- Would the organization go out of business?

This is the beginning of assessment, a critical first step for organizations wanting to reduce their risk using the CSCs. The first four Controls directly address risk, starting with fundamental processes such as inventory, implementation of secure baseline configurations, and assessment of hardware and software vulnerabilities:[3]

Critical Control 1: Inventory of Authorized and Unauthorized Devices

Critical Control 2: Inventory of Authorized and Unauthorized Software

Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Critical Control 4: Continuous Vulnerability Assessment and Remediation

Although each of the CSCs is important, the first two are the foundation for any serious approach to IT security; these four are seen as especially valuable by organizations such as the NSA, which rates them as "Very High" in their capability to mitigate attacks and "High" in technical maturity.[4]

---

2 www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf, p. 11

3 www.sans.org/critical-security-controls

4 www.sans.org/critical-security-controls/spring-2013-poster.pdf

Using the CSCs to Measure Risk

When considering how best to utilize the CSCs as a defense against data breaches, implementing them as documented is clearly the way to go. But as each organization integrates the CSCs into its own processes, it experiences an inevitable maturing as it musters the necessary time and resources. Executives and data owners alike must expect a lengthy period of transition during which they are still at least partially at risk from certain types of attack as they inventory and assess their systems against the perceived business risk discussed previously.

Organizations using the CSCs as guidance must be able to consistently measure themselves against the CSCs and quickly determine where the highest risk levels exist. Understanding which parts of the organization are subject to the most risk helps IT and line-of-business departments prioritize their remediation efforts and ensure that risks are remediated as quickly as possible with the resources and personnel available, with minimal disruption to operations.

Ideally, organizations will consider implementing software tools that executives and other business leaders can easily understand (in concept, if not actual use). The goal here is to help the bosses quickly understand the level of risk confronted by various facets of the enterprise at any given time. Comprehensive vulnerability management systems have the capability to identify weaknesses or vulnerabilities in systems and inventory risk across a large number of systems in an enterprise. This capability gives executives a clear picture of risk across all systems to help better prioritize their response. Dashboards from such tools, as shown in Figure 2, are often great first steps toward this objective if they are properly placed in the hands of business leaders, making them aware of the organization's true risks.

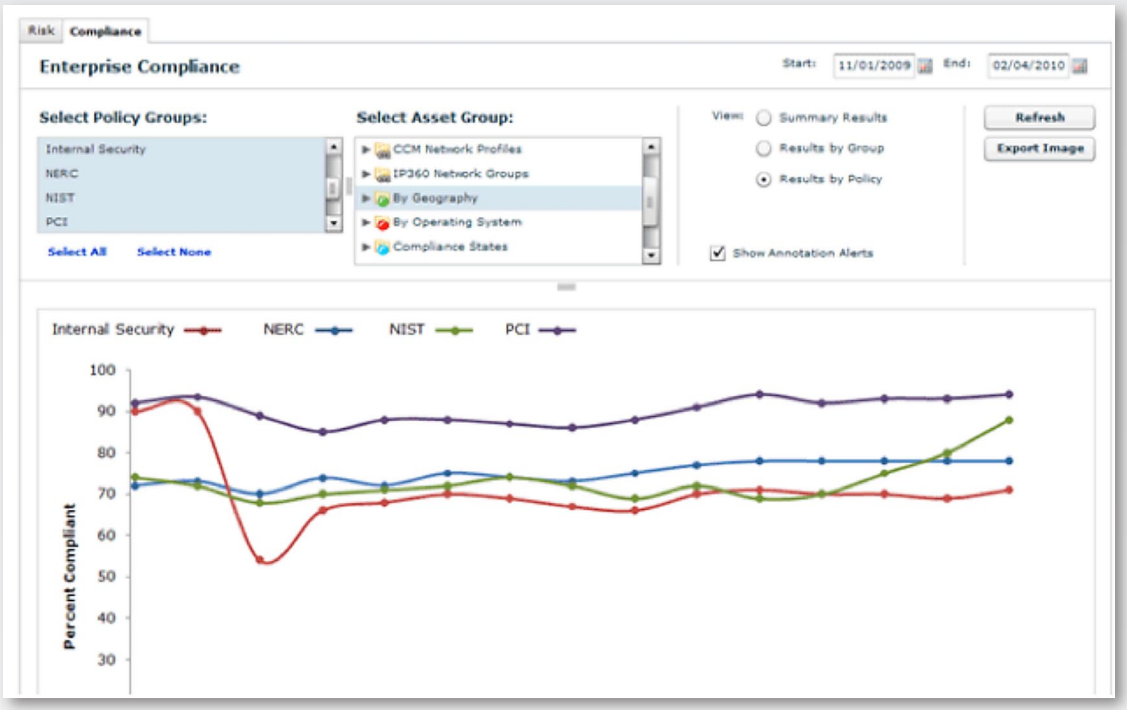

Figure 2. Example of a Vulnerability Management Dashboard for Executives[5]

5 www.ncircle.com/index.php?s=solution_reporting

In the short term, organizations should be self-aware and realistically assess their present capacity for risk mitigation.

No organization will have the resources to implement all of the CSCs at once. However, the first four CSCs reduce the capability of an attack to occur and spread, and they are often the controls organizations choose as a starting point. Implementing the full set of controls has turned out to be a long-term endeavor, requiring between three and five years to fully implement all of the CSCs. But in the short term, an organization may consider examining the first four CSCs as a baseline for vulnerability management dashboards that gather metrics such as the following:

- How many unauthorized or unknown computers are currently connected to the organization's network?
- How many unauthorized software packages are running on the organization's computers?
- What percentage of the organization's computers use software whitelisting defenses to block unauthorized software programs from running?
- What percentage of the organization's computers has been configured (OS and applications) according to the organization's documented standards?
- What is the Common Vulnerability Scoring System (CVSS)[6] rating for each of the organization's systems?

In the long term, business leaders must consider other questions as they comprehensively implement the CSCs. As they dedicate more quality time and quality effort to implementing this prioritized list, the metrics become increasingly meaningful; with meaningful metrics, business leaders will be better able to make sound business decisions that help the organization defend itself against data breaches.

Potential Outcomes of Attacks for Assessing Risk

Although it may be difficult to examine all the potential outcomes of a successful attack against your critical business systems, one can deduce the effects or impact at a high level. Although every possibility may be difficult to identify, one can also compile a list of the most likely outcomes. Business leaders need to understand that, of all the potential outcomes, the following are the most likely effects in the event of a breach:

- **Loss of data confidentiality.** If an attack were to succeed against an organization, one of the most likely outcomes is the disclosure of private or sensitive data. This might mean that sensitive business plans would be made available to adversaries, that confidential research and development notes would be available to competitors, or even that a client's data would now be available to adversaries. In most data breaches observed to date, this is the most common loss to an organization.
- **Loss of data integrity.** In other cases, but less commonly, the integrity of data is also at risk. Although the theft of sensitive business data is more likely than an attacker changing sensitive business information, the latter is still a risk. One common scenario where this could become an issue is a financial theft. The concern here would not be that someone would know *how much* money was in a bank account, but rather if they had the ability to *move* that money to another account, thus compromising the integrity of the account itself. This type of attack is generally of paramount importance to those in the financial services industry.

6 An open framework designed to help quantify IT vulnerabilities: www.first.org/cvss/cvss-guide.html

- **Disruption of service.** Another likely impact of an attack is some form of disruption of services. Although not the most common form of attack observed in the past 20 years, disruption of service is more likely than ever, thanks to the growth of hacktivism as well as an increasing number of nation-state actors. The most common example of such disruption is the loss of Internet connectivity, leading to clients being unable to interact with the organization, the organization's personnel being unable to perform a service and similar effects, but attacks in this category can range from a simple distributed denial of service (DDoS) that incapacitates an organization's website, to shutting down a manufacturing process,[7] to the disruption of financial services transactions.[8]

Each of these threats has the potential to disrupt normal business operations, so they must be taken seriously in any risk profile.

It should also be noted that, through proper project planning, resource allocation and prioritization based on CSCs 1–4, an organization could reduce the impact of these threats. This "planning for the worst" should occur in all spheres of business activity, whether that risk is of a power failure, disappointing sales or an Internet-based attack aimed at getting financial and customer data. With such foresight, the response to any such threats is a well-thought-out response to risk, one tailored to specific needs, rather than a reaction based on fear and hype.

7 www.darkreading.com/attacks-breaches/shamoon-saudi-aramco-and-targeted-destru/240006049

8 www.reuters.com/article/2012/09/21/us-iran-cyberattacks-idUSBRE88K12H20120921

Reducing Risk Through Preventive Security

Once an organization understands the threats it faces, it is then ready to understand the risk to potential target systems and users, and ultimately to take action to reduce its risk to defuse the threats.

One of the most common yet effective approaches to risk reduction is the "community risk assessment" model of security control selection, as defined by the CSCs. Developed in 2008 by the Center for Strategic and International Studies (CSIS), in partnership with the SANS Institute and multiple federal agencies, the CSCs address security challenges faced by enterprises and governments. According to CSIS:

> *This consensus document of 20 crucial controls is designed to begin the process of establishing [a] prioritized baseline of information security measures and controls that can be applied across federal [and] enterprise environments. The consensus effort that has produced this document has identified 20 specific technical security controls that are viewed as effective in blocking currently known high-priority attacks, as well as those attack types expected in the near future.*[9]

These organizations established the priorities with the help of more than 200 government and civilian groups, heavily influenced by feedback from the Department of State, the NSA, the Department of Cyber Crime Center (DC3), the Department of Energy, Australia's Defence Signals Directorate and other groups. The goal of the project was not to draft another to-do list, but to establish a new way of thinking aimed at helping organizations better defend themselves against Internet-based attacks, starting with identification and reduction of vulnerabilities that create risk.

Leveraging the research from such security groups will enable organizations to prioritize their defenses and proactively defeat their attackers through cleaner systems and better visibility and awareness of systems and system state. However, before an organization can hope to thwart its adversaries, it must understand their methods.

9 http://csis.org/files/publication/Twenty_Critical_Controls_for_Effective_Cyber_Defense_CAG.pdf

Dissecting a Compromised Company's "Kill Chain"

One of the most popular models of the methods dedicated attackers employ when attempting to compromise an organization's information systems is the "intrusion kill chain," first popularized in a 2010 paper by Lockheed Martin researchers.[10] Therein, the authors define a systematic approach that has been used with little variation by "professional-grade" hacking groups since 2005 (at the latest) to infiltrate and steal information from organizations around the world. Figure 3, based on the concepts described in the Lockheed Martin paper, illustrates the phases of these attacks.

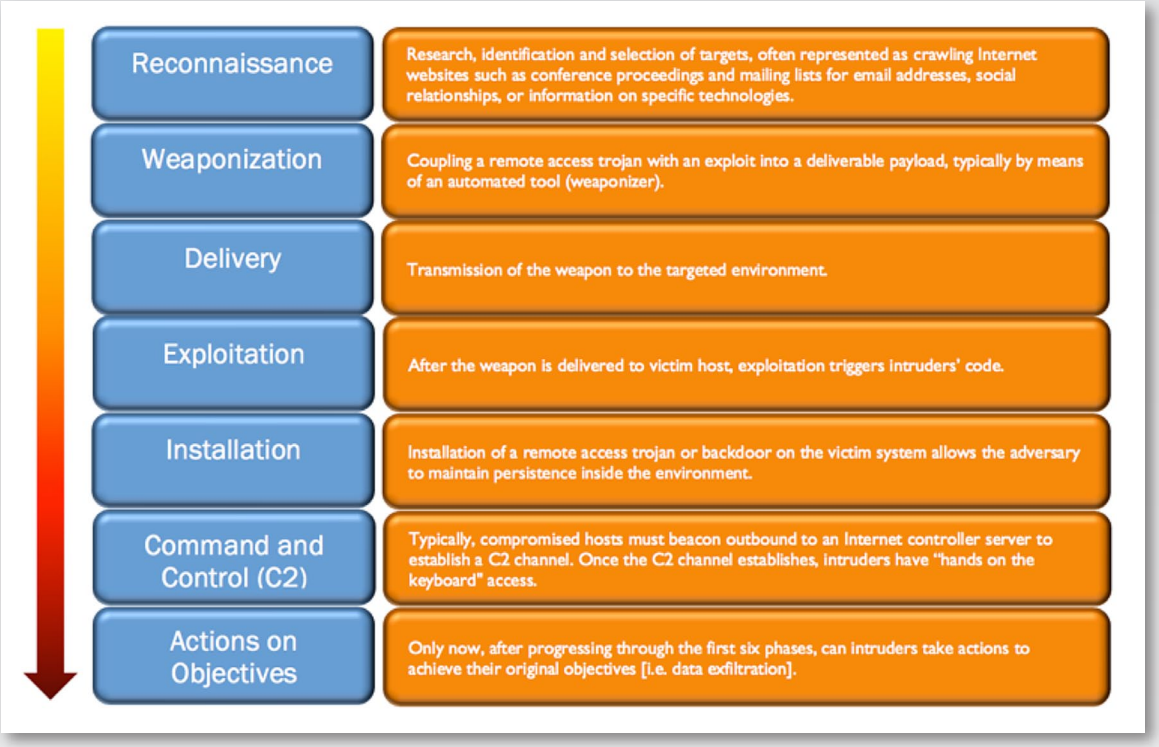

Figure 3. The Intrusion Kill Chain Model[11]

Data breaches do not "just happen." Rather, they are the results of weeks or months of planning, research and execution of detailed attack plans. Attackers do not randomly break into organizations' computers—they do so with specific intent; most every known computer attack witnessed in recent years had a purpose. Although that may vary (data theft, disruption of service, making a political statement, creating attack launch points and so on), the reality is that attackers no longer (or at least, rarely) compromise a company's IT systems simply for sport. In order to effectively achieve their goals, most attackers follow a model similar to the one illustrated in Figure 3.

10 Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, Ph.D., *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.* www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

11 Text from Hutchins, Cloppert and Amin. See Note 10.

Minimizing the Attack Surface with CSCs 1–4

The most important question to ask, therefore, is: What *can* organizations do to stop this sort of attack from being successful? If an organization's business goals include maintaining the confidentiality, integrity and availability of its data and its information systems, how can it achieve these goals? Although the hype says these goals are unachievable, a far more useful response is to identify the most likely threats and assign resources to combat them.

Each of the CSCs was included in the list of prioritized defenses to make it more difficult for an attacker to be successful. When implemented together, they act as layered defenses, giving organizations multiple opportunities to detect and prevent attacks as they occur, and when possible, *before* the attack can be launched. Although the entire point of defense is to keep attackers from being successful, too often these defenses are anything but state-of-the-art. Instead, they tend to be standard, "good hygiene" defenses that most organizations have been implementing to some degree for the last 20 years. One of the largest challenges organizations face in this area is the challenge of implementing the CSCs consistently across their environments—and in focusing on those CSCs that offer a high return on investment (ROI).

Getting Started with CSCs 1–4

Many organizations have chosen to implement these controls over a three- to five-year span, giving them realistic and achievable timeframes for securing various aspects of their information systems. It is important to note that the CSCs are ordered by priority, with Critical Control 1 being the highest priority, to give organizations the greatest chance for success.

In this spirit organizations frequently dedicate the first year of their implementation to the first four CSCs. These four complement each other and utilize many of the same approaches and technologies, making them a natural starting point for security initiatives. They are preventive in nature and, in terms of the intrusion kill chain, they focus on defending against attackers delivering, executing and installing attack code within the organization's information systems.

Although other CSCs are more "detective" in nature, attempting to stop an attacker from exfiltrating data from the organization, the first four Controls are focused instead on preventing the attacker from getting any toehold at all. For example, if an environment is fully inventoried, assessed and regularly (continually) patched and monitored for vulnerabilities, the attack surface shrinks considerably. Furthermore, if an attack was in progress and detected within an organization, a fully assessed environment would show which systems are at risk, and which are not. (In the next section, we present a specific example of how the first four Critical Controls can protect against the kill chain points in a known breach.)

Building a Layered Defensive Strategy

Another benefit organizations often achieve by implementing the first four CSCs in combination is the extra protection provided by layered or overlapping defensive technologies. By implementing fewer security systems that cover multiple endpoint types, or that backstop each other, organizations are able to achieve a large number of results. Specifically, organizations that deploy three classes of security systems can achieve significant compliance with the first four CSCs:

- A vulnerability management solution based on the Security Content Automation Protocol (SCAP)
- A system that monitors and assesses file integrity, enabling quick response to variances that may herald an intruder
- A software whitelisting solution

These systems, when integrated properly into an organization's alert management system and incident management practices, give an organization the capability to detect and prevent many of the attacks perpetrated in recent years, before an attacker is able to reach the end of the kill chain.

Kill Chain Case Study: 2013 Java Data Breaches

While theoretically discussing this problem is a good start, examining case studies of actual data breaches should give even greater insight into how this approach would be successful. A number of highly critical security flaws have just this year been revealed in Oracle's Java Runtime Environment (JRE); according to the National Institute of Standards and Technology (NIST), 91 unique vulnerabilities were disclosed in the JRE between the months of January and May 2013.[12] These vulnerabilities could allow an attacker to remotely compromise a victim who was running a vulnerable version of the software—most often through a link opened in a web browser.

To make matters worse, in February 2013 attackers showed that the use of Java as an attack springboard is an "in the wild" method of compromising computers. During that month alone, four major U.S. technology firms reported internal system data breaches resulting from vulnerabilities in Java. Twitter,[13] Facebook,[14] Apple[15] and Microsoft[16] reported almost identical internal data breaches; one must assume numerous other companies found themselves in similar situations, but simply did not report or even recognize the breach.

12 http://web.nvd.nist.gov/view/vuln/search-results?query=JRE&search_type=last3years&cves=on

13 https://blog.twitter.com/2013/keeping-our-users-secure

14 http://arstechnica.com/security/2013/02/facebook-computers-compromised-by-zero-day-java-exploit

15 www.reuters.com/article/2013/02/19/us-apple-hackers-idUSBRE91I10920130219

16 http://blogs.technet.com/b/msrc/archive/2013/02/22/recent-cyberattacks.aspx

In each situation the general attack pattern was identical:

1. The attacker discovered a weakness in software known or likely to be used by the victim. (Reconnaissance)
2. The attacker wrote attack code to exploit the discovered weakness. (Weaponization)
3. The attacker posted the attack code on a "watering hole" website that the victim would trust. (Delivery)
4. The victim was lured into visiting the "watering hole." (Exploitation)
5. The victim unwittingly downloaded and executed the attack code. (Installation)
6. The attack code compromised the victim's computer and connected to the attacker's command and control servers to facilitate the attacker's access. (Command and Control)
7. The attacker got what was wanted from the victim's computer (Actions on Objectives)[17]

As was discussed earlier, had any of the organizations mentioned comprehensively implemented the techniques documented in the CSCs, it would have had multiple opportunities to stop the attack during this intrusion kill chain. In particular, Critical Controls 1–4 could have prevented success of attack at various points in the kill chain. For example:

- **Critical Control 1 (Inventory of Authorized and Unauthorized Devices):** This control gives an organization a baseline of all authorized systems under their control. This level of visibility alone will help organizations quickly identify which systems may be impacted and—as importantly—which systems are not impacted by an event in progress. For example, if the Java attack was on Oracle systems but your organization is solely a Microsoft SQL Server shop, then no Oracle databases exist to be compromised. This is also the baseline control, ensuring that each of the other Critical Controls has been comprehensively implemented across all of the organization's devices—allowing for even better visibility device types and versions that might be involved in the attack.
- **Critical Control 2 (Inventory of Authorized and Unauthorized Software):** This control gives an organization an inventory of the software installed on each of its approved devices, including versions and state of the software. So in the Java example, this control enables the identification and updating of outdated versions of the Java application, stopping an attack before it reached step 5 (Installation) in the intrusion kill chain.
- **Critical Control 3 (Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers):** Adhering to this control means that each authorized system in the organization is configured according to approved standards and monitored for changes to those configurations. Had these organizations configured their systems to forbid Java code from executing via untrusted websites, they would have been able to stop the attack before reaching "Installation." Alternatively, had the malware changed a correctly configured system to reintroduce the vulnerability, that change would be noted, generating an alert in the monitoring dashboard.
- **Critical Control 4 (Continuous Vulnerability Assessment and Remediation):** As with Critical Control 2, had each organization been continuously scanning its systems for vulnerable software applications, it would have discovered the outdated versions of Java on its systems and been able to stop the attack, once again before reaching step 5 in the intrusion kill chain.

---

17 In each case the companies reported that they identified and stopped the breach before the attacker reached this point.

So, in the case of the Java exploit described, CSCs 1–4 would have worked on prevention and cleanup, as shown in Table 1.

Kill Stage	Attacker Action	Prevention Through CSCs 1–4
Reconnaissance	The attacker discovered a weakness in software known or likely to be used by the victim.	Inventory of applications and versions, patching and awareness of the patch level would protect against discovery of exploitable vulnerabilities on victim endpoint and in the database.
Weaponization, Delivery and Installation	The attacker develops a tool to exploit the discovered vulnerability and the end user.	Although not part of the first four CSCs, a healthy dose of training may help prevent success through social engineering. Vulnerability management of the endpoint would also be helpful in preventing initial foothold into the company.
Command and Control/ Exploitation and Spread	The attacker compromises victimized computer, sets up command and control facilities for the attacker, and seeks out the Oracle database for exploit.	All of these actions would create changes to the system that assessment tools should pick up and report on. System should also be able to show or prevent spread to other Oracle databases sought out by the attack code through visibility into all of its Oracle systems, including their state and patch level.
Mission Accomplished (Actions and Objectives)	The attacker has control of the target systems and the data within them.	Prevention through assessment and remediation really is the best protection. We will, however, need all of the CSCs to prevent, detect and minimize impact of events.

Table 1. The Kill Chain in Action

In short, had these organizations comprehensively implemented the first four CSCs, they would have been able to successfully defend themselves against these attacks and avoided the resulting data breaches.

Conclusion

In conclusion, Internet-based threats are real. Although there may be hype and confusion in the media about the nature and severity of many attacks, the reality is that the number of attacks grows with every year. Organizations simply cannot sit by and allow their information systems to be breached. They need to develop a practical strategy to prevent attackers from being successful. Through proper resource allocation and planning, these attacks can be mitigated through implementing the first four Critical Controls. Through the remaining CSCs, their spread can be stopped if an organization prioritizes its efforts on appropriate defenses, implementing related measures in steps, starting with device and system inventory.

The CSCs provide a "community risk assessment" for prioritizing defensive measures. With research and input from hundreds of U.S. government agencies and civilian contributors, it is a prioritized set of defensive measures developed specifically to reduce system risk, and make organizations more resilient to quickly detect and stop cyber attacks. Even if an organization cannot immediately implement each of these controls, at a minimum, if they can begin by implementing the first four CSCs, they will have moved a long way toward preventing these attacks from being successful.

With today's assessment and vulnerability management tools, the CSCs can be implemented with reasonable effort by any organization, small or large, and can provide measurements that are useful for understanding the current defensive state of an organization. With this information in hand, business leaders can be aware of the risks they face, as well as the severity of each risk. Armed with that knowledge, business and IT professionals in charge of system data availability and integrity can make better tactical and strategic decisions around their specific risk. They can also use the assessment capabilities they develop to benchmark their improvements and continually assess and assign risk, which is at the core of the CSCs, calling for continuous improvement in risk and response.

About the Author

James Tarala is a principal consultant with Enclave Security and is based out of Venice, Fla. He is a regular speaker and senior instructor with the SANS Institute as well as a courseware author and editor for many of their auditing and security courses. As a consultant he has spent the past few years architecting large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based, directory services, email, terminal services and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them in their security management, operational practices and regulatory compliance issues. He often performs independent security audits and assists internal audit groups with developing their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University (known today as Crain University) and did his graduate work at the University of Maryland University College, and he holds numerous professional certifications.

SANS would like to thank its sponsor: