Sponsored by
Tripwire and Patriot Technologies

Reducing Federal Systems Risk with the SANS 20 Critical Controls

April 2012

A SANS Whitepaper

Written by: G. Mark Hardy, CISSP, CISM
Advisor: James Tarala

Introduction

The United States is under attack. Our federal systems face unprecedented threats, and every federal employee is on the front line of this cyberwar.

Protecting our information systems is a top priority for all levels of leadership. The White House has budgeted $769 million for fiscal year (FY) 2013 (up from $459 million for FY 2012)[1] for the National Cyber Security Division of the Department of Homeland Security (DHS).[2] Teri Takai, Department of Defense Chief Information Officer, has a single quote on her homepage: "Information is our greatest strategic asset."[3] Her 10-Point Plan for IT Modernization emphasizes leveraging automated tools and continual assessments to strengthen cybersecurity.[4] At the RSA® Conference 2012, there was talk of U.S. and Canadian government agencies adopting the SANS 20 Critical Security Controls (20CSC) as a standard.

Potential cyber attackers are guided by many principles, some of them centuries old. The Chinese military strategist Sun Tzu wrote, "Speed is the essence of war. Take advantage of the enemy's unpreparedness; travel by unexpected routes and strike him where he has taken no precautions."[5] This strategy is a proven recipe for successful cyber attacks. As cyberdefenders, we must take precautions to prepare for these incidents. We, too, have principles and guidelines to orient our defenses. One of the best tools available for protecting federal systems is the 20CSC.

The 20CSC represent "a prioritized baseline of information security and measures and controls."[6] John Gilligan, former CIO of the U.S. Air Force and the U.S. Department of Energy, led the development of this document; it represents a consensus of government and nongovernment experts. It is not legislation, nor is it a formal government standard. Why, then, is this a better approach than the ten-year-old Federal Information Security Management Act (FISMA)? And how will adoption of the 20CSC ultimately enhance security and operations overall?

1 www.whitehouse.gov/omb/factsheet_department_homeland

2 www.whitehouse.gov/sites/default/files/omb/budget/fy2013/assets/homeland.pdf

3 http://dodcio.defense.gov

4 http://dodcio.defense.gov/Portals/0/Documents/ITMod/CIO%2010%20Point%20Plan%20for%20IT%20Modernization.pdf

5 http://en.wikiquote.org/wiki/Sun_Tzu

6 www.sans.org/critical-security-controls/cag3_1.pdf

FISMA and Other Legislation

When Congress passed the Federal Information Security Management Act of 2002 (FISMA, Public Law 107-347), it tasked federal agencies with developing and implementing agencywide information security programs. It was a good start, increasing senior management awareness and establishing a risk framework, but it also tended to establish a mindset of compliance—success was seen as the result of meeting annual reporting requirements. The Office of Management and Budget (OMB) estimated paper reports cost the Department of State about $1,400 per page to submit information that was often outdated within days.[7] Senator Tom Carper estimated that by 2009, the government had spent $40 billion related to FISMA.[8] In FY 2010, the federal government shifted to continuous monitoring and remediation of IT security vulnerabilities.[9] The White House directed agencies to submit monthly updates via Cyberscope, an automated tool, by November 2010.[10] FY 2012 reporting requirements remain unchanged from the previous year.[11] [12]

Although FISMA provides a structured approach to cyber risk management, its methodology can be considered administrative rather than operational—inventorying, categorizing, assessing, planning, certifying and accrediting. FISMA doesn't provide guidance on new technologies, nor does it reflect the increasingly interconnected nature of federal systems. Monitoring provides a measure of compliance, but not a robust set of defenses. Compliance has never guaranteed security. Dedicated adversaries repeatedly compromise systems that, on paper, have passed FISMA testing. Although FISMA serves an important purpose, it does not provide prioritized techniques for robust cyberdefense.

Congress has attempted to pass additional legislation to update FISMA, but these efforts have not always been successful. Consider the following efforts:

- House of Representatives Bill (H.R.) 4900, The United States Information and Communications Enhancement Act of 2009 (U.S. ICE Act) was introduced three years ago. It was intended "to recognize the interconnected nature of the Internet and agency networks."[13] This legislation had only two sponsors and died.
- Senate Bill (S.) 921, The Federal Information Security Amendments Act of 2010 (also known as "FISMA 2.0") also recognized the highly networked nature of the federal computing environment and provided a mechanism for improved oversight. However, this legislation died in committee.[14]

7 www.cio.gov/pages.cfm/page/Vivek-Kundra-Testimony-Federal-Information-Security

8 www.govinfosecurity.com/articles.php?art_id=1893

9 www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY10_FISMA.pdf

10 www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf

11 www.dhs.gov/xlibrary/assets/nppd/fism12-02signed.pdf

12 www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf

13 www.govtrack.us/congress/bills/111/hr4900

14 www.govtrack.us/congress/bills/111/s921

- H.R. 1136, the Executive Cyberspace Coordination Act of 2011, proposed the creation of a National Office for Cyberspace. It was referred to committee more than one year ago,[15] but has not yet reported out.
- H.R. 4257, the Federal Information Security Amendments Act of 2012, was introduced on March 26, 2012, by Rep. Darrell Issa of California. It lists essentially the same purposes as H.R. 1136, but because its sponsor is also the chair of the House Committee on Oversight and Government Reform, it is more likely this will be reported by committee to the full House. However, GovTrack estimates this bill has only a nine percent chance of passage by Congress.[16]

Thus, we see that Congress has made repeated efforts over the years to update and upgrade FISMA,[17] but until such legislation actually makes it into law, federal agencies will have to look to other sources for security leadership.

15 www.govtrack.us/congress/bills/112/hr1136

16 www.govtrack.us/congress/bills/112/hr4257

17 www.fas.org/sgp/crs/natsec/R42114.pdf

The SANS 20 Critical Security Controls

Most security practitioners are familiar with the 20CSC. The controls are designed to counter an adversary's actions of conducting reconnaissance, gaining access, keeping access and exploiting target systems by stopping attacks early, stopping multiple attacks, and mitigating the impact of any attacks that are implemented. The controls, listed in Figure 1, are prioritized by their capability to provide a direct defense against attacks. The first four controls have a very high effect on attack mitigation, while the last two are rated as having a low effect (but still important enough to be implemented.)

Critical Control	Effect on Attack Mitigation
1. Inventory of Authorized and Unauthorized Devices	Very High
2. Inventory of Authorized and Unauthorized Software	Very High
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Very High
4. Continuous Vulnerability Assessment and Remediation	Very High
5. Malware Defenses	High
6. Application Software Security	High
7. Wireless Device Control	High
8. Data Recovery Capability	Moderately High to High
9. Security Skills Assessment and Appropriate Training to Fill Gaps	Moderately High to High
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Moderately High
11. Limitation and Control of Network Ports, Protocols, and Services	Moderately High
12. Controlled Use of Administrative Privileges	Moderate to Moderately High
13. Boundary Defense	Moderate
14. Maintenance, Monitoring, and Analysis of Security Audit Logs	Moderate
15. Controlled Access Based on the Need to Know	Moderate
16. Account Monitoring and Control	Moderate
17. Data Loss Prevention	Moderately Low to Moderate
18. Incident Response Capability	Moderately Low to Moderate
19. Secure Network Engineering	Low
20. Penetration Tests and Red Team Exercises	Low

VERY HIGH — These controls address operational conditions that are actively targeted and exploited by all threats.

HIGH — These controls address known initial entry points for targeted attacks.

MODERATE — These controls reduce the attack surface, address known propagation techniques, and/or mitigate impact.

LOW — These controls are about optimizing, validating, and/or effectively managing controls.

*Figure 1: The 20 Critical Security Controls (Version 3.1) and Their Effect on Attack Mitigation (Adapted from **www.sans.org/critical-security-controls/winter-2012-poster.pdf**.)*

Note that the prioritized order is not necessarily the best order for implementation, nor does it represent logical groupings with respect to how security products operate. For example, some products address Critical Controls 3 and 10, whereas others may address Critical Controls 5 and 13. Figure 2 groups critical controls based on their applicability to the phases of adversary action to attack networks. Best practices consist of thoroughly assessing the risk posture of the enterprise and selecting the control sets that address the vulnerabilities with the greatest impact.

Categories of Attack Mitigation

Figure 2: Critical Controls and the Adversary Actions They Address
*(See **www.sans.org/critical-security-controls/winter-2012-poster.pdf**.)*

Federal agency chief information officers (CIOs) and chief information security officers (CISOs) contributing to the 20CSC document concluded that a prioritized baseline of information security measures and controls that are monitored automatically and continuously provide metrics is the only way to meet the needs of improved security controls and response. More than a checklist, the 20CSC is a compilation of real controls that make an operational difference. It is a "living document" in that updates reflect reprioritized controls based on current trends and the evolving threat landscape. The Center for Strategic and International Studies worked with the SANS Institute, Blue teams from the Department of Defense and other federal agencies, military investigators, and federal law enforcement officials and cybersecurity experts to develop these controls (see Appendix A for contributors and resources). The philosophy behind the controls can be applied to all environments, but federal system owners and operators can benefit particularly from this resource. Even the National Security Agency (NSA) is developing cybersecurity guidelines based on the 20CSC.[18]

Whereas FISMA is the law, the 20CSC represent best practices. No legal mandate for their implementation exists. Nonetheless, implementations in the real world have made a difference in the security status and culture of federal agencies. Let's take a look at a successful implementation of the 20CSC.

18 www.defensenews.com/article/20120116/DEFREG02/301160016/NSA-Crafting-Cyber-Guidelines

The 20CSC in Action at the U.S. State Department

Leadership is the key to influencing agencies to implement the 20CSC. The basic tenets of leadership include responsibility, accountability and authority. One of the difficulties facing federal CISOs and security managers is having the responsibility to implement security changes without the requisite formal authority. Thus, the effective security leader must master influence strategies that transcend positional authority.

As CIO of the U.S. State Department, John Streufert mastered this challenge by demonstrating more than a 94 percent reduction in measured security risk by implementing the 20CSC. He earned a 2010 Federal 100 award[19] and was promoted earlier this year to become the head of the Homeland Security Department's National Cybersecurity Division[20] (remember the $769 million budget mentioned earlier?).

His strategy was brilliant. Utilizing a custom application called *iPost*[21] that continuously monitored and reported on IT infrastructure risk, his team utilized the 20CSC to establish the Risk Scoring Program, which measured hosts, sites, regions and the entire enterprise. By establishing a dynamic score calculation based on criticality of component and issuing an easy-to-understand letter risk level grade from A+ to F-, he was able to provide each system administrator with frequent, consistent feedback in the form of a scorecard, as well as a list of the ten servers under that administrator's control that posed the greatest security risk. Key was establishing a grading system accepted as being fair to those evaluated—no penalty was assigned, for example, for a failure of a measurement tool to assess a particular system.

As time went on and scores improved, the grading scale was tightened to encourage continuous improvement. After all, once you earn an A, who wants to backslide to a B+? When the out-of-cycle Microsoft patch MS10-018 was released in late March 2010, by progressively raising the risk score for unpatched systems from 40 up to 320 points, Streufert motivated system administrators to achieve a 90 percent patch compliance rate in a single week (see Figure 3), whereas other federal agencies took months to reach only 20 percent to 65 percent compliance.[22]

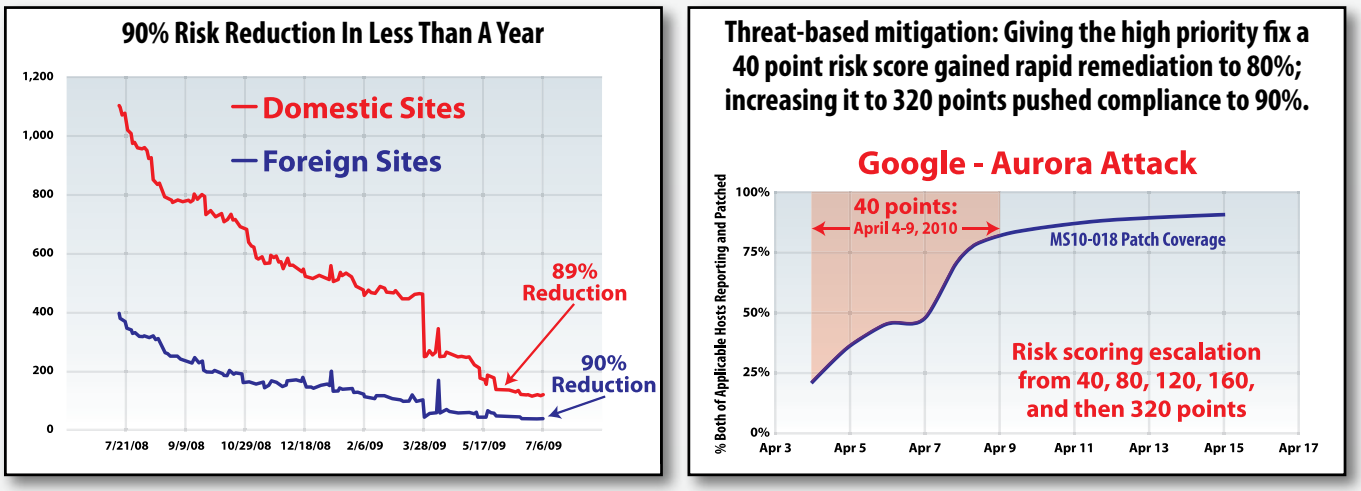

Figure 3: Raising the risk score motivated administrators to 90 percent compliance.
*(See **www.sans.org/critical-security-controls/winter-2012-poster.pdf**.)*

19 http://fcw.com/articles/2010/03/22/federal-100-streufert-john.aspx
20 http://blog.dhs.gov/2012/01/dhs-announces-john-streufert-as-new.html
21 www.state.gov/documents/organization/156865.pdf
22 www.sans.org/whatworks/20-critical-controls-poster-122010.pdf

A key lesson learned is that leadership should implement systems that can extract and abstract security data and align it with assets to provide a flexibility of views. Utilizing tool sets that show test and configuration failings along with a separate asset risk (by criticality) assessment can provide a clear picture of which systems should be remediated first from a risk perspective.

In short, data-driven automated metrics based on a prioritized list of controls (20CSC) and a realistic assessment of what administrators can control provided the cultural change that resulted in tremendous reduction of risk. These techniques can work for any agency if implemented thoughtfully.

Automation: The Key to Success

The 20CSC support the automated reporting requirements of FISMA. The controls are not organized randomly. Rather, they are prioritized based on an NSA assessment of control influence. This is a key concept. Agencies trying to meet FISMA requirements may feel overwhelmed with the scope and depth of requirements. 20CSC puts "first things first"—Critical Controls 1 through 4 are those rated very high in their capability to mitigate attacks. In addition, Critical Controls 1 and 2 are considered foundational—they form the baseline for a secure enterprise. This means agencies have a meaningful starting point for corralling the security of their systems.

This doesn't necessarily mean you should start with Critical Control 1 and work your way down. For agencies that have incomplete defenses, NSA recommends first implementing Critical Control 5 (Malware Defenses), Critical Control 8 (Data Recovery Capability) and Critical Control 9 (Security Skills Assessment and Appropriate Training to Fill Gaps). Note that the first 15 controls can and should be automated completely. Tools that provide for automation of the highest priority controls should be high-priority acquisitions for federal security managers.

Management Can Be Influenced by Security Success

The CISO of one of the largest Midwest power companies gave a talk at the Orlando SCADA Security Summit where he told the audience he had implemented the 20 Critical Controls and that, for the first time, senior management understood what needed to be done in cybersecurity. Based on his success, management guaranteed his budget so he doesn't have to fight for funds to fix security. On top of the extraordinary success with the 20 Critical Controls at the State Department, his story is another good reason why 2012 is a good time to implement the 20 critical controls. And that's especially true because of NSA's initiative to lead by example in implementing them.[23]

23 www.sans.org/newsletters/newsbites/newsbites.php?vol=14&issue=15&rss=Y

Critical Control Structure

Each of the 20 critical controls is subdivided into four specific categories: quick wins, improved visibility and attribution, hardened configuration and improved information security hygiene, and advanced implementation. For example, an organization implementing Critical Control 2, "Inventory of Authorized and Unauthorized Software," makes use of the following structure:

- Achieves a quick win for enumerating authorized software for each type of system
- Achieves improved visibility by deploying software inventory tools throughout the enterprise that tracks operating systems and applications by version and patch level
- Provides better configuration and hygiene results from deploying application whitelisting technology that uses acceptable hashing algorithms to determine authorized binaries (and code that has been inadvertently or maliciously modified)
- Uses an advanced technique to establish a trusted snapshot of a virtual machine that could be easily reloaded to client workstations

The controls also come with key metadescriptions that make them more "groupable" and actionable. For example, segmenting out all the controls that map to "NSA Manageable Network Plan Milestones and Network Security Tasks, Milestone 7: Baseline Management" creates a short list of controls that can be addressed by tools that provide baselines. Similarly, segmenting out controls that say "Sensor: File integrity software" will create a short list of two controls that can be addressed by the same type of solution (Critical Controls 3 and 10).

Thus, there is a structure within a structure, allowing federal security leaders to prioritize their efforts based on the maturity of their security program, as well as the availability of funding and resources.

Relationship to NIST

The National Institute of Standards and Technology (NIST) has been working to develop a unified information security framework for the federal government. As part of the Joint Task Force Transformation Initiative, NIST announced on February 28, 2012, the initial public draft of Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.[24] The first major revision since August 2009, this document is one of a series that lays out standards and requirements for implementing FISMA. Changes were driven by threats requiring greater attention, such as insider threat, mobile and cloud computing, and the advanced persistent threat (APT).

The 20CSC map extensively to the P1 Priority Code Security Controls in the 18 "families" listed in Appendix D of SP 800-53. For example, 20CSC Critical Control 1, "Inventory of Authorized and Unauthorized Devices" maps to Configuration Management control CM-8 (Information System Component Inventory), Program Management controls PM-5 (Information System Inventory) and PM-6 (Information Security Measures of Performance). Mapping is not one-to-many, but many-to-many—the many elements of both of these documents are intertwined. This mapping is important because changes in SP 800-53 may precipitate revisions to the 20CSC.

24 http://csrc.nist.gov/publications/PubsDrafts.html

Achieving Security on a Budget (or No Budget)

No agency has the funds to implement perfect security. Leaders must be creative and be good stewards of the resources entrusted to them to get the most value for the taxpayer. Russell Eubanks has written an outstanding paper, "A Small Business No Budget Implementation of the SANS 20 Security Controls."[25] It provides recommendations for implementing many of the 20 controls that utilize tools already embedded in operating systems such as Windows, as well as free and commercial products.

Naturally, you must remain within your agency's guidelines when pursuing security objectives, but the article includes many valuable concepts that can get you thinking in new directions. For example, for Critical Control 3, "Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers," can make use of the Microsoft Baseline Security Analyzer (MBSA), which was designed for small- and medium-sized businesses and can determine the security state of systems, including misconfigurations, and offer remediation guidance.[26] Also, security controls are not always as granular and segmented as the 20CSC list. For example, an organization employing integrity checking or change auditing tools can very often use them to satisfy large parts of Critical Controls 3 and 10.

As part of the Federal Desktop Core Configuration initiative, the U.S. Office of Management and Budget has required that "Information technology providers must use Security Control Automation Protocol (SCAP) validated tools, as they become available, to certify their products do not alter these configurations, and agencies must use these tools when monitoring use of these configurations."[27]

NIST provides a list of SCAP-validated products.[28] Some of these vendors offer no-cost trial versions for certain environments. The time spent becoming familiar with the resources available through this program is worthwhile.

25 www.sans.org/reading_room/whitepapers/hsoffice/small-business-budget-implementation-20-security-controls_33744

26 http://technet.microsoft.com/en-us/security/cc184923

27 www.cio.gov/documents/FDCC_memo.pdf

28 http://nvd.nist.gov/scapproducts.cfm

Conclusion

Security is rarely a matter of absolutes; it consists primarily of reducing risk to acceptable levels. Federal systems administrators face significant challenges with respect to securing their enterprise. The 20CSC represent a proven, prioritized set of processes and principles that work in the federal systems space. Here are steps you can follow to success:

- **Employ tools that provide an automated response.** Acquiring the right tools is essential to meeting monthly reporting requirements, as well as extending the span of control to meet the challenge. Systems are too extensive and complex to rely on manual methods. Utilizing tools that trigger deeper checks or take actions based on initial alerts will improve response time and reduce risk exposure. Further, automated systems reduce the opportunity for well-meaning workers to introduce error into the process.
- **Develop a strategy for implementation and follow it.** Start with the easy wins on the first several Critical Controls and build your security program from there.
- **Focus on the controls first and vendors second.** Some suite vendors seem to be able to provide all, or nearly all, of the 20CSC, but a one-vendor-fits-all approach often creates gaps. Focus first on how to best satisfy each control objective.
- **Master the art of influence.** Learn from others' successes. Follow examples such as those at the Department of State. Measurable change is achievable without formal authority.
- **Always maintain your guard.** You have a special trust to protect our nation's information systems from attack and compromise.

With the right tools and the proper initiative, every federal agency can achieve success in implementing the 20CSC for effective cyberdefense.

Appendix A

Contributors to the 20 Critical Security Controls Document

The following have contributed to the current version of the Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (20CSC):[29]

- Blue team members inside the Department of Defense (DoD) who are often called in when military commanders find their systems have been compromised and who perform initial incident response services on impacted systems
- Blue team members who provide services for non-DoD government agencies that identify prior intrusions while conducting vulnerability assessment activities
- U.S. Computer Emergency Readiness Team (CERT) staff and other nonmilitary incident response employees and consultants who are called upon by civilian agencies and companies to identify the most likely method by which systems and networks have been compromised
- Military investigators who fight cybercrime
- The FBI and other law enforcement organizations that investigate cybercrime
- Cybersecurity experts at U.S. Department of Energy laboratories and federally-funded research and development centers
- DoD and private forensics experts who analyze computers that have been infected to determine how the attackers penetrated the systems and what they did subsequently
- Red team members inside the DoD tasked with finding ways of circumventing military cyberdefenses during their exercises
- Civilian penetration testers who test civilian government and commercial systems to determine how they can be penetrated, with the goal of better understanding risk and implementing better defenses
- Federal CIOs and CISOs who have intimate knowledge of cyber attacks

Additionally, input from more than 100 other collaborators has been incorporated into the current version of this document.

Resources

Unified Information Security Framework for Federal Government

- *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (NIST Special Publication 800-37) – http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
- *Recommended Security Controls for Federal Information Systems and Organizations* (NIST Special Publication 800-53) – http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
- *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans* (NIST Special Publication 800-53A) – http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf
- *Managing Information Security: Organization, Mission, and Information System View* (NIST Special Publication 800-39) – http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
- *Risk Management Guide for Information Technology Systems* (NIST Special Publication 800-30) – http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Office of Management and Budget

- FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management – www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf

---

29 Taken from Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (www.sans.org/critical-security-controls/cag3_1.pdf), 8–9.

About the Author

G. Mark Hardy serves as president of National Security Corporation. He has been providing cybersecurity expertise to government, military and commercial clients for more than 25 years, and is the author of more than 100 articles and presentations. He serves on the National Science Foundation's CyberWATCH Advisory Board, and is a recently retired Navy Captain. A graduate of Northwestern University, he holds a B.S. in computer science, a B.A. in mathematics, a master's in business administration, a master's in strategic studies, and is designated as a Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM).

SANS would like to thank its sponsors: