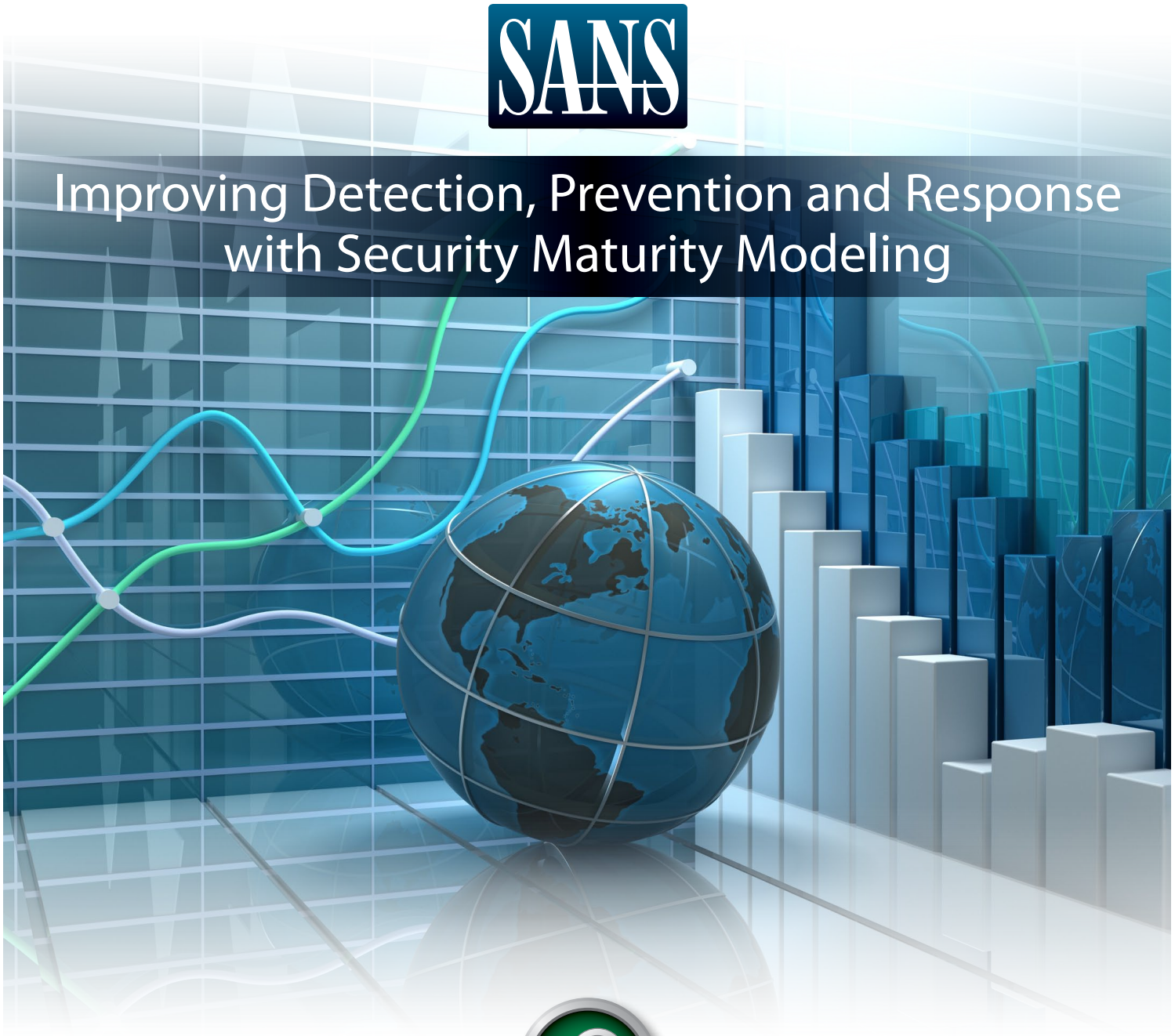
Interested in learning more about security?

SANS Institute InfoSec Reading Room

Improving Detection, Prevention and Response with Security Maturity Modeling

An Analyst Program whitepaper written by Byron Acohido. It discusses various security maturity models and how organizations can use them to improve their defense posture while reducing the time needed to respond to incidents and contain the damage.



Improving Detection, Prevention and Response with Security Maturity Modeling

A SANS Whitepaper

Written by Byron Acohido

Advisor: Tony Sager

May 2015

Sponsored by

HP

Introduction

A burgeoning underground is systematically plundering and disrupting IT networks. Waves of attacks against organizations' endpoints, applications and networks are so pervasive that they are forcing organizations to focus on improving their security and response programs.

As witnessed by a variety of large breaches to go public in 2014 and 2015, a major network breach can result in the loss of intellectual property and personal data, customer and shareholder lawsuits, even compliance audits and sanctions. Fallout from a network breach more often than not is proving to be material, judging from the record 783 data breaches made public in the U.S. in 2014, a 30 percent increase over 2013, as tracked by the Identity Theft Resource Center.[1]

Although a bottom-line damage figure is impossible to derive, the aggregate damages to breached organizations appear to be in the billions of dollars annually. The so-called Carbanak hacking gang alone has been tied to advanced persistent threat (APT) attacks against 100 banks of all sizes that have netted the criminals an estimated $1 billion over the past two years.[2] Meanwhile, analysts estimate it will cost Target more than $1 billion to fully recover from losing payment card transaction records for 110 million customers.[3]

If damage from an advanced network-based attack can be material, then taking cost-effective steps to understand and reduce the exposure is logical and prudent for all organizations.

This paper outlines a basic approach to maturing security operations and, in the process, making security more cost-effective while improving risk posture. Those just waking up to security, as well as organizations looking to refine and steadily improve existing security programs already in place, can benefit from maturing their programs to concentrate on measurable outcomes.

[1] "Identity Theft Resource Center Breach Report Hits Record High in 2014," Jan. 12, 2015; www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html

[2] "Bank Hackers Steal Millions via Malware," *The New York Times*, Feb. 14, 2015; www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html

[3] "Analyst sees Target data breach costs topping $1B," *Prairie Business*, Jan. 31, 2014; www.prairiebizmag.com/event/article/id/17645

This fundamental approach derives from a formal process, known as capability maturity modeling (CMM), that organizations have used for years to improve their cybersecurity posture. CMM increases the effectiveness and efficiency of security programs by focusing on thorough and repeatable security processes that can self-improve, become more automated and become integrated into the overall operational infrastructure. By moving from "chaotic" processes (i.e., those that are reactive and not interconnected) to maturing and continually improving processes, enterprises can increase the level of security delivered to the business at the point where it's needed while reducing spending through measurable improvements and efficiencies.

The most mature security programs focus on integrating security controls into architectural approaches that increase security while reducing risk and the costs and breakage experienced in reacting to ever-changing threats. In contrast, the least security-mature organizations may have just installed their first firewalls or IDSes.

Most organizations fall somewhere between the extremes of the maturity curve. This paper explains the key components of this model and provides resources to help organizations improve their security posture regardless of their point on the maturity curve.

Many forms of maturity models exist, the most well-known example having been started by the U.S. Department of Energy (DOE) and then removed of sector specifics so that other industries can use it.[4] CMM increases the effectiveness and efficiency of security programs by focusing on thorough and repeatable security processes, recurring risk analysis studies, threat monitoring and documentation, and compliance auditing.

Measuring Improvements

Capability Maturity Model (CMM) and Capability Maturity Model Integration (CMMI) are registered trademarks of Carnegie Mellon University (CMU) that apply to software, integration and engineering.[5] CMMI identifies five measurement areas that should be considered in such a program, providing case studies to illustrate each area, including the following:

- Cost
- Schedule
- Quality
- Customer satisfaction
- ROI

Despite the many different models even within CMMI, the CMMI FAQ site says the general philosophy behind all CMMI models is the same:

> *"CMMI is a model … from which (astute) organizations will abstract and create process improvement solutions that fit their unique environment to help them improve their operational performance."*[6]

By maturing from an ad hoc approach to a pattern of continually improving business processes, organizations can increase the overall level of performance while simultaneously reducing growth in spending. For example, a study of 12 use cases in systems integration, engineering and software development conducted by Carnegie Mellon University showed measured improvements in cost, scheduling, quality (reducing defects), customer satisfaction and ROI through the CMMI model. Specifically CMU cited a 33 percent decrease in cost to fix a defect, as well as a 20 percent reduction in unit software costs. In addition, one case study reported a savings of up to $2 million just six months after improving its CMMI processes and procedures.[7]

[4] "Cybersecurity Capability Maturity Model, (February 2014)," U.S. Department of Energy website; http://energy.gov/oe/downloads/cybersecurity-capability-maturity-model-february-2014

[5] "Demonstrating the Impact of CMMI: An Update and Preliminary Results," (Carnegie Mellon University) Software Engineering Institute website, http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=6365

[6] CMMI FAQ website; www.cmmifaq.info

[7] "Demonstrating the Impact of CMMI," pg. 7

CMM is a model that fits naturally with all enterprise IT security processes, starting with software development.[8] But CMM does not apply solely to development. The basic framework of CMM can be utilized as a generalized roadmap for measuring and improving any organization's entire IT security posture, regardless of how far along it is in the maturity process. For example, take the core elements of the model:

- **Cost.** In the case of an overall security maturity model, the point would be to reduce the cost of events occurring or attempting action on your network.
- **Schedule.** This means detecting events sooner and remediating them accurately and efficiently.
- **Quality.** Remediation should also include full repair of the vulnerabilities exploited and improved response to similar events.
- **Customer Satisfaction.** IT security should be seen as a business enabler rather than an obstacle to achieving objectives.
- **ROI.** Although the key goal is to reduce the cost and complexity of risk management and response, mature security can include charge-back revenues from business units.

Leading tech consultancies have started weaving CMM components into scoring models, and vendors are including maturity measurement capabilities in their services and interfaces. Some good resources include the ESG Cybersecurity Maturity Model, which outlines people, processes and technologies behind such a model, and Gartner's ITScore for Information Security for organizations to self-diagnose their maturity levels.[9]

[8] "What is Capability Maturity Model (CMM)?" TechTarget; http://searchsoftwarequality.techtarget.com/definition/Capability-Maturity-Model

[9] The ESG model is described in "What's Your Security Maturity Level?" from *Krebs on Security*, April 15, 2015; http://krebsonsecurity.com/2015/04/whats-your-security-maturity-level/; Gartner's IT Score, at "ITScore for Information Security," June 21, 2013; www.gartner.com/doc/2507916/itscore-information-security

Measuring Maturity

All of these models describe basic levels of the maturity curve. For example, in software CMM, TechTarget describes the key measurements of security maturity using the same methodology from Gartner's ITScore-based assessment guide that encompasses business processes, technology and tools, business culture, as well as personnel and organization.

In this case, the first step toward improving any organization's security posture begins with an understanding of what a very basic security maturity curve looks like. The next step is to approximate where the organization sits on that curve and then, of course, begin to proactively pursue improvements.

In its report, Gartner goes on to further describe these various stages:

Level 1: Initial. The enterprise's management is aware that information security is weak and represents unacceptable risks. Information security activities are ad hoc and typically IT-focused. In most cases, no formal information security program is in place.

Level 2: Developing. An individual has informal responsibilities comparable with those of a chief information security officer (CISO), who is working to develop program plans and policies. Different stakeholders are beginning to communicate informally about information security issues.

Level 3: Defined. Policies and rules are in place and some information security roles and responsibilities are established, but there is little accountability or enforcement. Information security efforts are still primarily IT-focused, and enterprise security awareness is still limited.

Level 4: Managed. Information security roles and responsibilities are clearly defined, and a formal information security committee—led by the CISO, with participation from the line-of-business managers—is operating. The enterprise is moving away from an IT-centric approach to information security, but line-of-business owners have not yet accepted explicit accountability for residual risk.

Level 5: Optimizing. Line-of-business managers have now explicitly accepted the residual risk associated with their use of information and technology, and they are fully accountable for security failures and policy violations. Continuous self-improvement practices are in place, regularly updated and used to create a security-aware culture in their organizations.

Figure 1 shows a typical progression of information security score levels using the Gartner ITScore model.

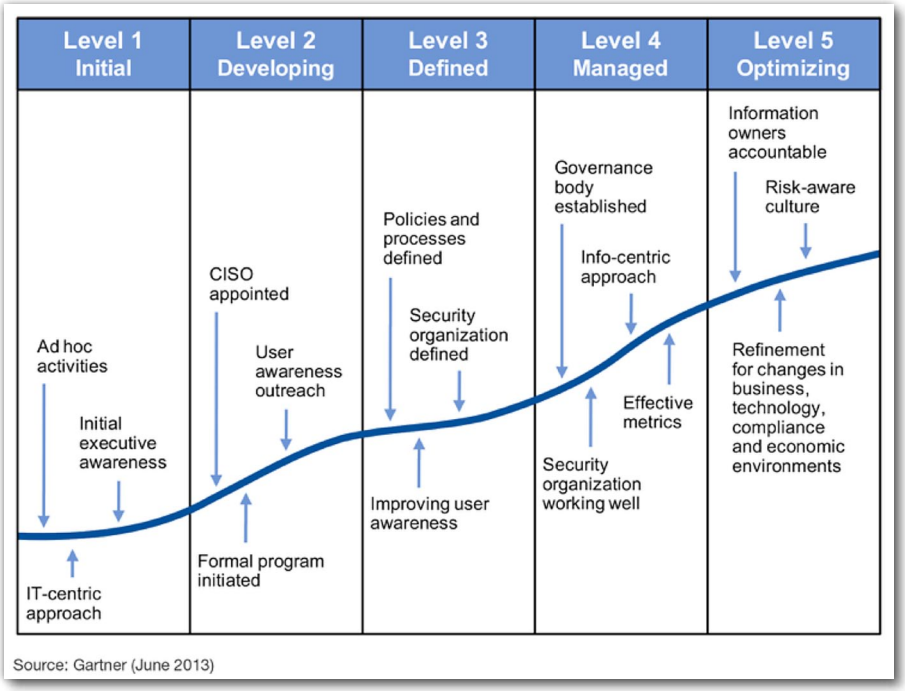


Figure 1. Gartner-Defined Information Security Score Levels[10]

Identifying Immature Traits

According to the ESG report, immature organizations are ignorant of cybersecurity issues or they do the minimum required, often based on headline-driven assumptions. When a database is compromised or a website gets corrupted or defaced, actions are taken on an ad hoc basis and very little is documented, let alone repaired or improved upon.

Organizations at the lower end of the maturity curve typically have ill-defined processes and procedures, and they acquire and implement security technologies and services in a decentralized manner, typically in response to a specific attack or in a unilateral effort to comply with regulations.

[10] "ITScore for Information Security," June 21, 2013; www.gartner.com/doc/2507916/itscore-information-security

There may be a CISO (or a person performing CISO functions), but that person reports to the IT director and routinely defers to IT's priorities. The company might even operate its own security operations center (SOC), but it has not truly integrated security controls into its network architecture. The SOC is poorly managed and generally disrespected.

Thus the efforts of security staffers get diluted due to misaligned expectations and competing priorities. What security budgets they have are susceptible to erosion. In a field where there is a shortage of skilled security technicians, a high level of attrition can reverse the maturity process and create a deteriorating security environment.

Recognizing Signs of Maturity

In maturing organizations, business, IT, security and response are aligning. They have started implementing formal security benchmarks that align with an organization's business goals. They document operational processes and procedures so actions leading up to, during and after a security incident can be repeated.

Maturing organizations also address compliance requirements, often informally, with changes triggered reactively rather than proactively. They remain highly dependent upon individual contributors and struggle to avoid dumping IT and administrative chores on staffers who should be dedicated to security tasks.

The CISO of a maturing organization often reports to the chief operating officer (COO), with a degree of autonomy from the IT director, according to the ESG report. However, resources are still scarce and retaining skilled staff remains a big challenge. Although rules are in place, senior management's information security concerns drive progress, and properly trained staff is available to support them.

How does an organization embark on the journey of steadily improving its security posture? One way is to follow a course laid out in some detail by the DOE in its 2014 Cybersecurity Capability Maturity Model (C2M2) report.

Make Frameworks Count

Many of the resources cited in this paper include documentable levels of maturation. For example, the DOE's C2M2 document lays out a flexible approach to building security models based on a combination of existing standards, frameworks, programs and initiatives and organized into 10 groupings of security practices, or "domains."[11]

C2M2 categorizes practices within a given domain by target objectives that support the domain. The C2M2 domains are as follows:

- Risk management
- Asset, change and configuration management
- Identity and access management
- Threat and vulnerability management
- Situational awareness
- Information sharing and communications
- Event and incident response, continuity of operations
- Supply-chain and external dependencies management
- Workforce management
- Cybersecurity program management

[11] "Cybersecurity Capability Maturity Model (C2M2)," U.S. Department of Energy website; http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity

Each set of practices represents activities that can lead to mature capability in their domains, while management objectives are to detect repeatable processes and practices across domains, as shown in the model depicted in Figure 2.

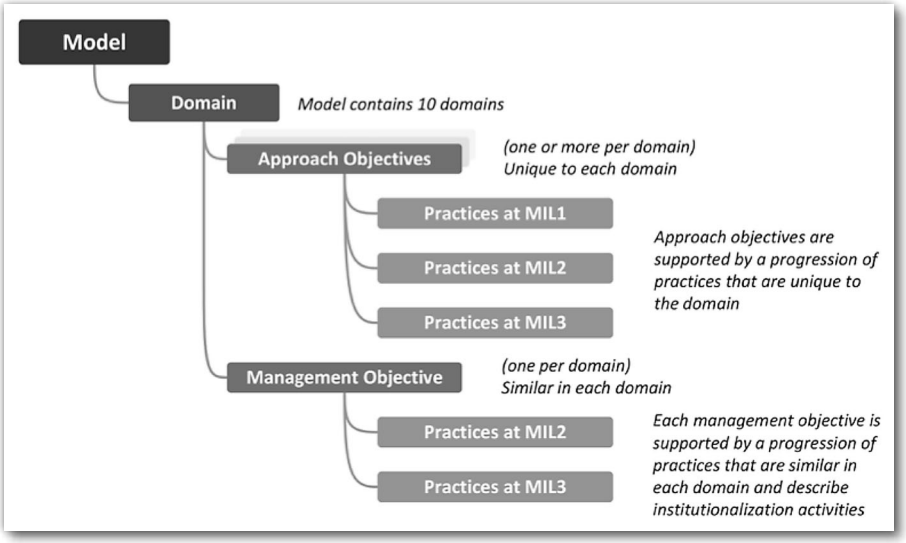


Figure 2. Elements of the DOE's Domain-Based C2M2 Model[12]

Assembling this template was no small task for the DOE, and implementing it in a live environment can be challenging. That's because CMM originally focused on a single chore: improving software design and build quality. However, as the C2M2 document vividly depicts, cybersecurity encompasses a much broader array of variables, most of which are problematic, at best, to directly control.

Start with Diagnostics

Organizations are embarking on and finding real savings in continuously monitoring for vulnerabilities and making improvements based on findings from their assessments, according to a 2014 SANS survey on diagnostics and mitigation.[13] The Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program provides federal government agencies with resources to identify and prioritize cybersecurity risks on an ongoing basis.[14] The program revolves around providing government networks and systems adequate, risk-based and cost-effective cybersecurity.

[12] "Cybersecurity Capability Maturity Model (C2M2)," U.S. Department of Energy website; http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity

[13] "Continuous Diagnostics and Mitigation: Making it Work," August 2014; www.sans.org/reading-room/whitepapers/analyst/continuous-diagnostics-mitigation-making-work-35317

[14] U.S. Department of Homeland Security website; www.dhs.gov/cdm

CDM provides tools that help agencies identify and prioritize cybersecurity risks and thus help security personnel triage perceived threats. The processes of continuous assessment and improvements represented in this program are already resulting in measured improvements in security and risk posture. For example, 44 percent of respondents to the SANS diagnostics and mitigation survey were able to measure improvements in their security, mostly through increased procurement efforts, but some experienced reduced costs of security improvements, as shown in Figure 3.[15]

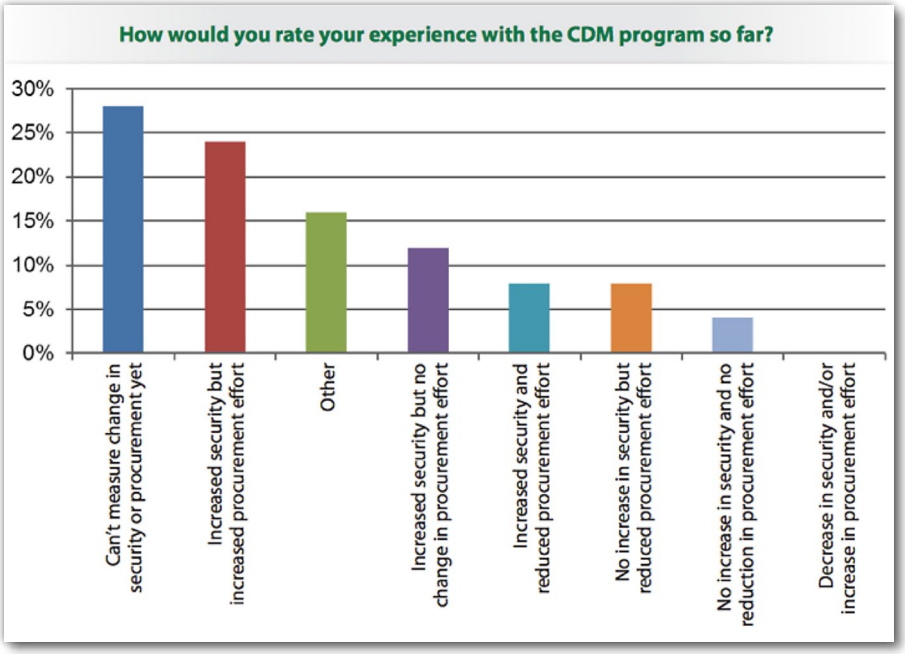


Figure 3. Measured Improvements with CDM

[15] "Continuous Diagnostics and Mitigation: Making it Work," pg. 17; www.sans.org/reading-room/whitepapers/analyst/continuous-diagnostics-mitigation-making-work-35317

CDM depends upon a continuous loop of keeping sensors up to date, automation, triage, repair and report, as shown in Figure 4.

Figure 4. Continuous Assessment, Reporting and Improvement Loop from CDM[16]

The program starts with the initial gap assessment, which 51 percent of respondents to the SANS survey said they were able to do. It then follows with departmental input, analysis, prioritization of repairs, repairs and updates of sensors to detect new forms of vulnerabilities, and progress reports.

Taken together, these key practice areas not only reduce attack surface, but they also integrate intelligence into future vulnerability detection processes and even prevention processes through sensors.

[16] U.S. Department of Homeland Security website; www.dhs.gov/cdm

Automate Processes

Although the CDM primarily focuses on government systems, the Critical Security Controls (CSCs) reach beyond the government and apply to all sectors looking to improve their risk management posture and measure their improvements. Like the CDM, the CSCs also focus on automation and integration.[17]

The CSCs are being widely adopted across all industries, particularly financial and government sectors, according to a 2014 SANS survey.[18] The CSC criteria were put together in 2009 by a consortium that included the NSA, United States Computer Emergency Readiness Team, Department of Defense, and other agencies, along with the top commercial forensics experts and penetration testers that serve the banking and critical infrastructure communities. Coordination was under the purview of the SANS Institute. Stewardship has since been transferred to the Center for Internet Security, an independent, global non-profit entity committed to a secure and open Internet and is continually updated.

In addition to prioritizing security functions, the CSCs outline standardization and automation processes proven to gain operational efficiencies while also improving effectiveness. This is accomplished via actions that are essentially a subset of the National Institute of Standards and Technology (NIST) SP 800-53.

Vetted by a broad community of public and private security experts, this smaller subset of actionable controls serves as the basis for immediate high-value action. Therefore, the CSCs are something any organization committed to improving its security posture could use to advance security maturity. Think of the CSCs as a basic guide for quickly and materially improving an organization's security posture in a very cost-effective manner. Key tenets of the controls include assessing gaps in security, tools and practice, as well as auditing and reporting implementation progress. Specific steps in the CSCs include the following:

- Inventorying authorized and unauthorized devices and software used inside the organization.
- Standardizing configurations on company laptops, servers and workstations with an eye toward streamlining vulnerability management.
- Monitoring incoming and outgoing LAN traffic to prevent exfiltration of valuable data.
- Analyzing audit logs, administrative privileges, malware defenses and data loss prevention and data recovery capabilities.
- Automating and using information collected to continuously improve security processes and reduce risk.

[17] "Critical Security Controls Now at CIS!" Center for Internet Security; www.cisecurity.org/critical-controls.cfm

[18] "Critical Security Controls: From Adoption to Implementation," September 2014; www.sans.org/reading-room/whitepapers/analyst/critical-security-controls-adoption-implementation-35437

Figure 5 lists the Critical Security Controls.

Figure 5. The Critical Security Controls

This information represents a body of intelligence that security analysts can use to reduce attack surfaces and detect events faster and more accurately for timely response and repair, driven by automated workflows.

Look Outward with Intelligence

Any organization starting at any level of maturity can always learn more and improve steadily over time. If your organization is not ready or prepared to implement a full-blown C2M2-type initiative, you can implement a much more basic approach to steadily improve your organization's security posture, one that holds true to the core principles of CMM. This basic approach is based on the notion that maturity correlates to an organization's capacity to utilize its own measurements of security and risk posture. The organization is also looking farther in space and earlier in time: Threat Intelligence helps network defenders learn from global threat activities beyond the view of their own sensors and before they impact systems within the enterprise.

"Threat Intelligence needs to be done as part of a designed, ongoing cycle of info gathering, assessment, use/ remediation, and feedback—that's really the value of the CDM program. Otherwise, more intelligence is just more noise."

-Tony Sager, SANS director

Tools Provide Intelligence

Most organizations, even very immature ones, already do this at a base level, by virtue of the fact that off-the-shelf security tools and services gather intelligence from globally dispersed sensors and use them to improve their security products and services. This intelligence is built into the heuristics and signatures of mainstream endpoint protection and antivirus suites, next generation firewalls and unified threat management systems (UTMs) and intrusion prevention technologies.

In a very real sense, these vendors are looking far beyond any single client's immediate assets and dynamically incorporating global intelligence in real time to improve immunity (detection) and remove vulnerabilities as they're discovered.

Manage Users

Some of these tools must include the ability to profile and look into user behavior, detect unusual actions and alert the appropriate people. These tools need to, as much as possible, automate the process of user awareness and education, as well as enforcement against bad actions.

User awareness makes it into the second (Developing) and third (Defined) stages of the Gartner maturity curve shown earlier in this paper. The ultimate goal, at level 5 (Optimizing), is to have a risk-aware culture that holds information owners accountable for their security.

Although many organizations are in the second stage of the Gartner model, they still struggle with their users and consider them a primary vector of successful attacks, according to many SANS surveys. For example, in the SANS 2014 survey on financial services security practices, "abuse or misuse by internal employees or contractors" was the top reason for their security incidents, followed by spearphishing emails—another form of user mistake.[19]

[19] "Risk, Loss and Security Spending in the Financial Sector," Table 1 (pg. 8); March 2014; www.sans.org/reading-room/whitepapers/analyst/risk-loss-security-spending-financial-sector-survey-34690

Sharing Intelligence

User behavior and other monitoring tools can and should provide intelligence for tracking suspect actions and reporting on them. Therefore, intelligence sharing is also critical to the growth and maturity of security and response programs.

Short of launching a full-blown C2M2, a fundamental way to embark on this journey is to participate in community-based security initiatives, the prime example being sector-specific information sharing and analysis centers (ISACs).

The stated mission of the National Council of ISACs is to:

> *Advance the physical and cyber security of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and with government. Members of the Council are the individual Information Sharing and Analysis Centers (ISAC) that represent their respective sectors.*[20]

ISACs originate from a simpler, less dynamic era. Officials from critical infrastructure key resource (CIKR) organizations thought it wise to convene periodically, typically once a quarter, to discuss security, share intelligence and learn from the experience of others in their respective sectors. Human interaction in such settings tapped into the power of relationships and common bonds, and a level of trust became engrained.

ISACs have emerged across more than a dozen sectors as trusted entities and sources of comprehensive sector analyses, intended to be shared within the sector, as well as with other sectors and with the government. ISAC services that can aid maturity include the following:

- Risk mitigation
- Incident response
- Alert and information sharing via briefings
- White papers, threat calls and webinars
- Anonymous CIKR owner/operator reporting
- Access to a 24-7 security operations center

[20] National Council of ISACs website; www.isaccouncil.org

The represented sectors include the following:[21]

- Aviation Information Sharing and Analysis Center ISAC (A-ISAC)
- Defense Industrial Base ISAC (DIB-ISAC)
- Emergency Management & Response ISAC (EMR-ISAC)
- Electric Sector ISAC (ES-ISAC)
- Maritime Security ISAC
- Multi-State ISAC (MS-ISAC)
- Communications ISAC
- National Health ISAC (NH-ISAC)
- Nuclear Energy Institute (NEI)
- Oil and Gas ISAC (ONG-ISAC)
- Public Transit ISAC (PT-ISAC)
- Real Estate ISAC (RE-ISAC)
- Research & Education ISAC (REN-ISAC)
- Supply Chain ISAC (SC-ISAC)
- Surface Transportation ISAC (ST-ISAC)
- Water ISAC

Face-to-face meetings are invaluable for sharing information, sharing best practices and conducting response exercises. Standardizing, sanitizing and automating the threat information for dissemination on a sector-by-sector basis also occurs within these ISACs. Some ISACs are also advancing along their own maturity curve, from talking about adopting automation standards (described later in this paper), creating rapid response systems and automated analytics, and sharing hubs. For example, the Financial Services ISAC (FS-ISAC) has a real-time sector alert feed system for members, informed by members.[22]

Thanks to a 2015 executive order calling for private sector entities to share cybersecurity threat information with one another as well as with the U.S. government, the level of threat intelligence provided through these groups, if shared and digested properly among industry organizations, should continue to reduce attack surface and aid in early detection and response (key tenets of maturing the security model).[23]

[21] "Member ISACs," www.isaccouncil.org/memberisacs.html

[22] Financial Services ISAC website; www.fsisac.com

[23] "Obama signs executive order on sharing cybersecurity threat information," The Washington Post, Feb. 12, 2015; www.washingtonpost.com/blogs/post-politics/wp/2015/02/12/obama-to-sign-executive-order-on-cybersecurity-threats

Shorten Response Time

One limitation of human collaboration is human speed. In today's threat landscape of botnets carrying out automated attacks at scale, quick and automated actions are required to adjust on the fly to stay ahead of the latest criminal practices. Sophisticated, well-funded intruders use the latest zero-day exploits to operate under the radar of mainstream defenses for extended periods. These events are driving organizations to demand a quicker, more accurate response time—something that takes more than a week, based on responses to a 2014 SANS incident response (IR) survey.[24]

As an organization moves up the maturity curve, automating response and reducing time to remediate becomes more critical. However, the diversity of security systems looms as a major obstacle to automation. Respondents to the SANS IR survey cited lack of time, budget and visibility across systems as their primary inhibitors to improving their incident response programs—all of which point to a lack of integration and automation.[25]

Look to Standards

Another collaborative, community-driven effort—the Structured Threat Information Expression (STIX) language—is in the vanguard addressing this bottleneck. STIX is an effort to define, develop and popularize use of a standardized language to represent structured threat information, putting sensor readings into a machine-readable format designed to capture threat indicators. STIX enables a scenario whereby if you see a certain file, with a certain date and hash, you can be fairly certain it's malicious.

> *The STIX Language intends to convey the full range of potential cyber threat information and strives to be fully expressive, flexible, extensible, automatable, and as human-readable as possible. All interested parties are welcome to participate in evolving STIX as part of its open, collaborative community.*[26]

STIX uses Trusted Automated eXchange of Indicator Information (TAXII) as the transport mechanism for threat information. TAXII is the means by which organizations can securely share cyberthreat information in near-real time.

Organizations ready to advance up the maturity curve can participate in the ongoing standards-making efforts for STIX and TAXII. Additionally, they can help accelerate wide adoption by insisting security vendors incorporate STIX and TAXII into tools and services.

[24] "Incident Response: How to Fight Back," August 2014, pg. 18; www.sans.org/reading-room/whitepapers/incident/incident-response-fight-35342

[25] "Incident Response: How to Fight Back," pg. 12

[26] STIX website; http://stix.mitre.org

Conclusion

Over the last two years, there has been an unprecedented level of breach disclosures in the U.S., led by the major attacks at Target and elsewhere. With cloud and mobile computing accelerating, an imperative clearly exists for any organization doing business in the Internet-centric global economy to seek to become more security-mature. Understanding the basic security maturity curve and gauging your organization's approximate position on that curve is the first step.

The next step is to begin proactively pursuing advancements in security maturity. It will take buy-in from senior leadership, line-of-business managers and any staffer using IT services to conduct company business. The good news is that tried-and-true CMM principles are supported and reinforced by government and industry initiatives such as C2M2, CDM, CSC, STIX and TAXII.

By proactively participating in and availing themselves of such models, organizations will make substantive incremental progress up the security maturity curve. This basic approach should put them on better footing to make decisions about security technology and services purchases from leading vendors and consultancies, many of whom are likewise striving to make security maturity models more digestible for organizations of all sizes. As seen from the software security maturity model, following this model would naturally produce efficiencies and cost savings for organizations as they progress up the curve.

About the Authoring Team

Tony Sager is the director of the SANS Innovation Center, which provides on-site IT security training for government and military organizations. He is a founding member and chief technologist of the Council on CyberSecurity, where he leads development of the Critical Security Controls, an international consensus project whose goal is to design and teach practices to counter the most pervasive forms of cyber attack. Tony spent more than three decades developing cutting-edge security as chief operating officer of the Information Assurance Directorate that provides the NSA's own IT defenses. He also led the NSA's first efforts at developing open security standards.

Byron Acohido is editor-in-chief of ThirdCertainty.com, a news and analysis website dedicated to helping businesses and individuals better understand emerging exposures and embrace best practices. Before launching ThirdCertainty last fall, Acohido covered technology, cybersecurity and privacy at *USA TODAY* for 13 years.

Sponsor

SANS would like to thank its sponsor:

Last Updated: April 22nd, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Blue Team Summit & Training 2018	Louisville, KYUS	Apr 23, 2018 - Apr 30, 2018	Live Event
SANS Riyadh April 2018	Riyadh, SA	Apr 28, 2018 - May 03, 2018	Live Event
SANS Doha 2018	Doha, QA	Apr 28, 2018 - May 03, 2018	Live Event
SANS SEC460: Enterprise Threat Beta Two	Crystal City, VAUS	Apr 30, 2018 - May 05, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, ILUS	May 01, 2018 - May 08, 2018	Live Event
SANS SEC504 in Thai 2018	Bangkok, TH	May 07, 2018 - May 12, 2018	Live Event
SANS Security West 2018	San Diego, CAUS	May 11, 2018 - May 18, 2018	Live Event
SANS Melbourne 2018	Melbourne, AU	May 14, 2018 - May 26, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VAUS	May 20, 2018 - May 25, 2018	Live Event
SANS Amsterdam May 2018	Amsterdam, NL	May 28, 2018 - Jun 02, 2018	Live Event
SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
SEC487: Open-Source Intel Beta Two	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
Cloud INsecurity Summit - Washington DC	Crystal City, VAUS	Jun 08, 2018 - Jun 08, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
Cloud INsecurity Summit - Austin	Austin, TXUS	Jun 11, 2018 - Jun 11, 2018	Live Event
SANS Oslo June 2018	Oslo, NO	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS ICS Europe Summit and Training 2018	Munich, DE	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, JP	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Crystal City 2018	Arlington, VAUS	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Philippines 2018	Manila, PH	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Cyber Defence Canberra 2018	Canberra, AU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Malaysia 2018	Kuala Lumpur, MY	Jul 16, 2018 - Jul 21, 2018	Live Event
SANS Seattle Spring 2018	OnlineWAUS	Apr 23, 2018 - Apr 28, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced