N.J. Division of Revenue and Enterprise Services

Security for the Networked Enterprise, Elements of a Holistic Approach

January 2018

Abstract

This research paper, developed by James Fruscione, Director of the New Jersey Division of Revenue and Enterprise Services, covers the basic elements of a multi-faceted, holistic security program for organizations employing networked information technology (IT) platforms. The paper includes an introduction that explores the multiple dimensions and impacts of the cyber threat terrain, and highlights the need for strong security programs in networked environments. The main section of the paper deals with common components of computer security programs and the aligned techniques, tools and operational features that promote detection, prevention and control of security threats/risks. Other sections touch upon network-accessible data and overall IT asset protection methods. The intellectual model for the paper is based on normative and prescriptive frameworks that outline security best practices and guidelines. Of particular significance here are the frameworks set forth by professional consortia such as the SANS Institute, Federal agencies like the National Institute for Standards and Technology and international entities, particularly the International Standards Organization. References to scholarly and industry-based works supplement the discussion on the frameworks. The goal of the paper is to augment understanding of the institutional and technical dimensions of sound security programs in contemporary networked computing environments through discussion of elements that apply to virtually all network-connected systems. The paper should not be construed as a policy directive from the State of New Jersey. Additionally, the paper does not endorse any specific commercial security solutions or platforms.

Keywords: computer network security, technology security framework, information asset protection

Security for the Networked Enterprise, Elements of a Holistic Approach

Introduction

Computer-based resources and processes, and the networks that connect them, are the virtual nerve centers of our business, social, economic and political systems (Coupey, 2005). These automated resources, processes and networks serve as conduits for our legal, financial and commercial interactions, and deliver vital governmental information and services to the public. They also undergird our national defense, public safety, healthcare and infrastructure programs, and allow for social, cultural and political engagement on a global scale, unbound by time and geography (Coupey, 2005; Laudon & Laudon, 2014).

Viewed in this context, computer-based resources are key digital assets, which facilitate our collective progress toward the attainment of prosperity, health and security – here in the United States and internationally. Equally true, however, is the fact that these digital assets have become targets for nefarious actors who seek to mine automated systems and aligned communications networks for illicit and harmful purposes. These purposes include identity theft, fraud, espionage, defacement, disruption and/or destruction of our information system infrastructures (Laudon & Laudon, 2014). In the dark worlds of cyber criminality and geopolitical conflict, computer-based systems become both the agents of their own degradation, and their aligned communications networks become the pathways through which attacks and stolen assets travel. Thus, just as digital assets propel humanity along a positive trajectory, their misuse engenders deleterious outfalls of significant negative proportions. The Infosec Institute catalogs some of these outfalls, including loss of intellectual property, privacy intrusions, brand image/reputation degradation, employment loss, and personal/business financial losses (2013-The Impact, 2013).

The threats to digital assets emanate from multiple sources and are dynamic and ever-evolving. For example, criminals, terrorists, activists and adversarial nation states seek to exploit computer-based resources, processes and networks through vectors that touch virtually every aspect of information technology architectures (2013- The Impact, 2013). Exacerbating this situation is the fact that attacks could originate from internal threats. That is, employees with criminal or unethical intentions may introduce threats directly into the organization's systems or do damage to the physical facilities that house the systems. Alternately, through negligence or ignorance, employees may fail to heed warnings about unsafe online behavior or fail to protect digital assets under their custody, thus leading to security compromises and data loss (Behm, 2003).

Software-based attacks may travel from outside networks located across the globe – most especially through Internet connections, and enter organizational networks via electronic mail, file exchanges, web site interactions or other electronic touch points. These attacks can implicate network infrastructures and/or all forms of network-connected resources such as servers, data storage fabrics, firmware appliances and end user devices such as desk top computers, notebook computers, smart phones and tablets (2013- The Impact, 2013). Compromised devices introduce malware such as Trojans, worms, viruses and remote control programs (botnets), which affect vulnerable application and operating system software, and data storage platforms. These intrusions, in turn, may lead to information loss, hijacked processes and/or disruption, defacement or destruction of information systems (Laudon & Laudon, 2014).

Given the factors above, it seems clear that organizations involved with the creation, acquisition, movement and management of digital assets must take strong measures to protect them – to institute security programs that guard the core integrity of these assets. This security

imperative is apparent in the legal and regulatory frameworks that mandate protective measures for networked computer systems, IT systems and digital assets in general. Behm (2003) outlines several of the most important elements of the legal and regulatory landscape here. He highlights laws and regulations that require Federal government agencies to address IT security controls – for example, the Federal Information Security Act (FISMA) and Office of Management and Budget's Circular A-130, and other laws and regulations that prescribe various obligations to protect digital assets in the public and private sectors. The latter include the US Privacy Act and the Health Insurance Portability Accountability Act (HIPAA). Other acts, such as Sarbanes-Oxley and Gramm-Leach-Bliley, mandate security-related measures for digital assets and information managed by private sector entities, while industry-driven compliance regimes such as the Payment Card Industry Data Security Standards (PCI-DSS) require stringent controls for commercial transactions conducted via digital channels (IT Compliance, 2015).

As can be inferred from this brief introduction, the scale, complexity and implications of cyber threats are extensive and multi-dimensional. They implicate virtually every aspect of IT infrastructures, especially networked platforms. Legal and regulatory requirements that mandate measures to protect digital assets formally articulate the need to respond to these security threats. For both practical and legal reasons then, organizations must plan for and institute security programs for their networked and general IT resources. One could argue that to be successful in such endeavors, organizations must scale their programs to meet the multi-dimensional cyber security challenges that face them, and be prepared to extend these programs to cover the entire range of digital assets across the enterprise. In this regard, they must eschew unidimensional approaches that focus only on segments of their networked complexes or on programs that center too heavily on technical tools or procedural controls. Instead they must strive to institute holistic

programs that cover the full range of technical and institutional elements that meet the multi-dimensional threat environment in a comprehensive fashion.

To help shed light on what is involved in creating and maintaining a holistic security program, the following discussion outlines and discusses key IT/network security elements. It touches upon both the basic institutional aspects of a holistic program and the aligned technical tools, techniques and operations that support a strong security posture. The intellectual model for the discussion is based on the normative and prescriptive security program frameworks published by the SANS Institute, the National Institute of Standards and Technology (NIST) and the International Standards Organization (ISO) (Information Technology, 2009; Framework, 2014; Critical Security Controls, 2015). References to scholarly and industry-based works supplement the discussion of the framework elements. Other security regimes such as PCI-DSS and Safeguard (IRS standards for managing Federal tax information) are not included, but arguably, the three general frameworks used here are broad enough to cover the core elements that transaction- and asset-specific standards/guidelines include. Also, while the paper does not cover third-party Cloud services or facilities management arrangements directly, much of the discussion is relevant to and can be helpful in the construction of service level clauses for these contract-based models.

Institutional Elements

The following discussion outlines the roles, functions and organizational resources that are typically associated with a multi-faceted, holistic networked computer security program. Several academic works and standards publications serve as the basis for the discussion.

Roles, Budgetary Support and Project Management

While varying factors such as organizational size, mission, environmental complexity and financial resources shape the unique staffing patterns of a given organization, it is logical to conclude that in order to meet the pressing challenges of network and IT security, all organizations must have clearly delineated roles for the security function. Indeed, without focused managerial attention on network and overall IT security, it is hard to envision any organization being able to sustain the integrity of its vital informational resources (Behm, 2003). In this regard, the Laudons (2014) highlight that security roles typically fall under a chief technology officer (CTO), who in turn may work with a Chief Information Security Officer (CISO). The CTO focuses on planning for the overall development, maintenance and protection of the organization's IT infrastructure and systems, while the CISO concentrates specifically on infrastructure and data security.

Ideally, the CTO and CISO work with an organization's executive management team to develop a strategic vision and agenda for the organization's security program, which are based on structured methodologies such as the asset classification and risk assessments discussed below. Also, the vision and agenda can be translated into measures generally known as key performance indicators (KPI). In a security environment, these measures serve to communicate how well the organization's security program performs relative to program goals/objectives set forth by the CTO/CISO (Rouse, 2006). Security KPI can be: project management-related such as the degree to which the organization delivers security program projects on time, within budget and with the functions specified in the project scopes of work; and functional – for example, average time taken to escalate and resolve security alerts and to respond to notifications of variances from security baselines such as unexpected spikes in outbound network traffic volumes

and use of non-standard end user device configurations (Tate & Martin, 2010; Critical Security Controls, 2015).

Relative to the strategic agenda, the CTO and CISO are responsible for structuring, presenting and securing the budgetary resources needed to run daily security operations and services. Further, these managers are responsible for developing capital project plans for the organization's security infrastructure (major, long term upgrades and enhancements) and for managing these initiatives through to completion (Behm, 2003; Laudon & Laudon, 2014). In this connection, project management efforts involve the use of tools and techniques that document the scope of projects, monitor/report on progress against schedules, verify the delivery of specified outputs (deliverables), and track/control project expenses versus budgets (Tate & Martin, 2010).

Collectively, the institutional roles and budgeting and project management elements discussed above form the institutional foundations for holistic security programs. They are the focal points for leadership, vision, managerial responsibility and financial support that drive incisive planning, security infrastructure development, implementation of security policies/procedures, and application of key security techniques/tools on a consistent basis.

Governance

Closely aligned with the institutional roles above is information governance – that is, the development and enforcement of policies aimed at fostering a responsive IT infrastructure, and within this area of concern, sustaining the organization’s network and IT security posture, most especially with regard to the daily actions of employees and stakeholders (Laudon & Laudon, 2014). Generally, CTOs and CISOs use two foundational policies in this area – information and acceptable use policies.

Overall, the information policy outlines the organization's requirements for managing data assets and employee responsibilities for handling data through its life cycle (from capture/creation through to use, management and disposition) (Laudon & Laudon, 2014). With specific regard to security, Bayuk (2009) notes that the security-related aspects of the organization's policy should cover elements like classification of data resources (see Asset Classification/Risk Assessment below), policies/procedures regarding privacy, credential protection (for example, prohibitions against sharing passwords), non-disclosure provisions (for proprietary data), etc.

The acceptable use policy adds depth to the general information policy. It stipulates to employees and stakeholders with access to the organization's digital assets that both information technology equipment and software, along with data created and/or maintained by the organization, are the organization's property. It also spells out password creation and protection requirements, reinforces confidentiality/privacy rules, prohibits using organizational resources for personal or illegal purposes, bans misuse of the network itself (for example, unauthorized port scanning or downloading of unauthorized software), outlines proper use of electronic mail and other forms of electronic communications that flow through the network, and specifies the consequences of non-compliance (Acceptable Use, 2009).

Security-related Training and Education

As can be inferred from the discussion on governance above, it is vital for employees to be mindful of the security imperative, especially as it relates to networked data and IT infrastructure resources. Put directly, employees must have the knowledge and skills required to comply with the organization's security regime. To this end, mandatory and frequently updated training and education programs are developed to cover the key areas of concern. For instance,

written and/or online presentations can be structured to: instruct programmers on safe coding techniques such as those that prevent the exposure of log-in credential and sensitive parameters and error messages online; educate general end users with respect to safe Web browsing practices and the tell-tale characteristics of risks like phishing attacks; and inform system administrators relative to methods for evaluating event and system logs (Critical Security Controls, 2015). The organization can supplement these internal training/education efforts by funding substantial outside educational programs that focus on targeted instructions on network and IT security provided through academia and/or industry groups.

Asset Classification and Risk Assessment

In order to align security measures with networked and general IT assets in an effective and efficient fashion, it is important for organizations to have a view of the relative value of these assets and their potential exposure to security lapses, damage and loss. In this connection, organizations can apply asset classification and risk assessment techniques to help prioritize investments in security-related resources, and to shape the scope of the security program.

Asset classifications may cover both network and IT infrastructure/data resources. The classification process encompasses an inventory of assets. For infrastructure assets, this includes documenting the number and location of end user devices, servers, firmware appliances, network switches/routers, network operating systems, database systems, application software, etc., and their significance to the organization's core operations, brand and compliance posture. The significance of the assets can be expressed on a scale -- for example, high (essential), medium or low (Standards for Security, 2004). For data assets (all data stores administered by the organization), the focus is on determining the locations and custodians of the assets, and ascertaining whether a given asset is confidential or proprietary. The data asset inventory also

involves deciding on the required levels of availability (tolerance for loss, damage and/or delayed access) and integrity or trustworthiness that must be maintained (Standards for Security, 2004).

With a classification scheme in hand, organizations can execute risk assessments by juxtaposing the relative value of the assets -- for example essential and confidential data that must be available 24x7 versus low value reference data that do not require high availability, against a threat matrix that details potential security issues and the likelihood/impact of their occurrence. Threats that are likely to occur and that impact high value assets constitute key vulnerabilities, and therefore merit heightened attention and substantial allocations of security program resources (Framework, 2014).

When viewed in the context of risk, one can see that networks and network-connected assets are vital considerations for organization seeking to institute holistic security programs, most especially organizations that must interact with the public and partners through the Internet and other external connections. Put simply, opening internal networks and network-connected resources to these external communications channels exposes the organization's IT platform to the global reach of criminals, hostile nation states and other nefarious actors who are intent on disrupting, damaging and/or stealing resources from targeted systems (Behm, 2003; Critical Security Controls, 2015). This fact establishes the actionable and compelling context within which organizations apply the security-related tools, techniques and operational features later in this paper.

Auditing

The final institutional element centers on an on-going audit regime. Generally, the regime involves the use of trained IT security auditors -- internal audit staff and/or consultants from

third-party firms, who review the security program and practices on at least an annual basis for compliance with: the organization's governance requirements (standards and procedures); applicable laws and regulations; and best practices. The result of the audit effort is a report that outlines the overall status of the program, findings relative to deficiencies and variances from required policies, procedures, laws and regulations, and recommendations for remedial actions (Fennelly, 2003). The concept here is to maintain vigilance and to obtain actionable information that enables the organization to respond to signs of program lapses and/or trends that indicate the need for new or upgraded practices that strengthen the security program.

Tools, Techniques and Operational Features

This section highlights various security-related software, hardware, procedures and operational components needed to cover the interconnected assets that make up a networked computing environment. The main sources of information for this part of the paper are the security program frameworks published by professional groups such as the SANS Institute, Federal agencies like the National Institute for Standards and Technology and international entities, particularly the International Standards Organization. Scholarly and industry-based works supplement the discussion and references to specific technologies offered by the industry help to illustrate how the security-related tools techniques and features are implemented.

Intellectual Control (Mapping Information/Network Infrastructures)

Building from the asset inventory discussed earlier, the mapping exercise encompasses documenting all servers, routers, switches, bridges, storage fabrics and end-user devices that form, and interconnect with, the organization's network. It also includes all software operating within the network complex – operating/database systems and business application software (Information Technology, 2009; Framework, 2014; Critical Security Controls, 2015). At base,

the goal here is to gain intellectual control of the map, and based on this control, to ensure that only authorized devices and software programs can connect to and access the organization's digital assets. Significantly, the mapping activity also connects with the governance and classification concepts discussed above, and includes active monitoring/follow up to remove unauthorized/unmanaged hardware and software that appear on the map (Harris, 2006).

The significance of the threats posed by unauthorized hardware and software provide a strong incentive for organizations to implement mapping programs. The SANS Institute notes that hackers and persons with malevolent intent from virtually every corner of the globe actively scan networks to find and exploit attached hardware that is not consistently patched/updated with appropriate security features, or that is not properly configured with strong passwords and role-based access levels (Critical Security Controls, 2015). The Institute also observes that cyber-attacks may focus on outdated and vulnerable versions of software, including browsers that visit sites infected with malware hidden in web pages, links, documents and rich media files. Once compromised, a single device or program can propagate malware through the organization's network and cause various, serious issues ranging from service disruptions to data breaches and compliance gaps, through to catastrophic system failures (Pironti, 2005).

To address this aspect of the control regime, organizations require software tools like Microsoft's System Center Configuration Manager (SCCM) to perform network-wide scans for attached hardware and software programs, and to provide alerts whenever an unauthorized device or program is detected (System Center, n.d.). This functionality must extend to mobile devices that attach to the network. Further, the organization will need to institute procedural and/or automated controls for individuals who periodically attach notebook computers and

mobile devices to the network, which ensure they install the latest software patches and security updates before navigating to organizational data sources or external web pages (Pironti, 2005).

Security-Hardened Configurations

This aspect of the program also complements the asset inventory processes described previously. Quite simply, IT equipment and software products of all kinds are delivered with configurations that are designed primarily to facilitate installation/implementation, and are thus replete with security gaps that hackers may exploit, such as: generic passwords; open services/ports (access points that are easy targets for hackers); unpatched and/or outdated operating system/application software versions; and unneeded applications (Framework, 2014; Critical Security Controls, 2015).

With respect to network devices themselves, default settings such those described above are also prime targets for hackers and criminals. Exploitation of default settings can lead to unauthorized system access via routers and switches – devices that direct data transmissions. Ironically, the same problem could affect firewalls, which are specifically designed to prevent the propagation of unwanted and illicit network traffic (Information Technology, 2009; Framework, 2014; Critical Security Controls, 2015). Exploitation of network devices is especially troublesome because compromised nodes can be manipulated to redirect traffic and/or permit interception of high value/sensitive information, thereby providing the foundations for data corruption or theft (Behm, 2003).

To address configuration issues, organizations implement procedures and systems that convert unsafe firmware and software settings to secure organizationally-approved states (golden or standard images) for use throughout their networks. Controls in this area are designed to establish *and* maintain stable images. This means that organizations must adopt automated,

systematic and rigorous patching/updating processes to ensure that the latest malware protections are installed and operational at all times (Laudon & Laudon, 2014). Other actions in this area center on constructive responses to the default configuration issues noted previously. Here, organizations remove original installation accounts, close open ports and disable and/or delete unneeded software/services (Framework, 2014; Critical Security Controls, 2015). Moreover, organizations will need to consider running domain name, file share, electronic mail, database and other vital services on separate physical or logical servers. The SANS Institute notes that this provides for higher levels of visibility, segregation and control of key network-connected resources (Critical Security Controls, 2015).

With regard to network devices and programs like firewalls, routers, and switches, organizations can compare their configurations with standard, secure configuration parameters, and make any changes needed to bring the device configurations into conformance with the required settings (Framework, 2014; Critical Security Controls, 2015). Also, as with other IT equipment, organizations must monitor for changes made to network devices and respond rapidly if non-conforming changes or anomalous activities are detected (Casey, 2013).

Tiered (Multi-level) Network Defenses

Because threat vectors are numerous and ever-evolving, it seems clear that even with strong mapping and configuration programs, organizations are not impervious to intrusions and compromises. Threats emerge and change too rapidly and involve too many variables. So, it is not safe to assume that mapping and configuration programs alone provide for a flawless, sustained state of protection. It behooves organizations, therefore, to design their networks in a way that insulates core IT and informational resources such as mission critical data bases, content stores and business software applications, from devices and processes that interact with

external networks -- most especially the Internet, which is the primary source of external threats (Information Technology, 2009; Framework, 2014; Critical Security Controls, 2015).

Organizations can achieve a high degree of insulation by employing a tired or multi-level network defense structure with multiple layers of firewalls. Firewalls are implemented in both hardware and software, and they help to block out communications streams to/from unsafe venues. For example, they filter out unwanted traffic by examining inbound and outbound data packets based on rules the organization establishes, and block unauthorized flows based on these rules, including data flows that carry the indicia of problems (Avila, n.d.). Various vendors, including CISCO, Fortinet, CheckPoint Software Technologies and Sophos, offer enterprise level firewall products (Hils, Yound & D'Hoine, 2015)

In tiered network defense configurations, firewalls may be deployed at various points in the architecture. For example, they may be employed simultaneously at the external boundary of the network -- the point at which the organization's routers connect with external networks (including the Internet), and at points between the external boundary and Internet (Web) servers (commonly called the DMZ). In turn, there may be a firewall between the DMZ and zones containing Web database servers, and finally, firewalls between the latter zone and core production data bases (Ferro, 2009; Laudon & Laudon, 2014).

To complement the layered firewall protections, and further insulate IT resources, the SANS Institute recommends that organizations configure all client devices so that they send service requests to Domain Name Servers (DNS) on their internal networks (intranets) and never to DNS located on the Internet (Critical Security Controls, 2015). Likewise, it would be prudent to position firewalls in front of servers that run mission-critical business applications to block the

ingress and egress of unauthorized network traffic from the resource (Ferro, 2009; (Critical Security Controls, 2015).

Finally, organizations could divide their networks into smaller trust or security zones (network-connected resources that share functional, geographic, confidentiality or other common characteristics), each with their own firewalls and security regimes. The idea here is to extend the depth of security and at the same time, prevent the entire network from being compromised if one of the zones is impacted by a cyberattack (Grimes, 2010).

Anti-Virus/Anti-Malware

These software-based defense products run on network connected devices and general IT equipment, including end user computers. They detect, quarantine and remove malware such as Trojans, worms, viruses and other malicious code designed to disrupt services, steal data, highjack control of system resources and/or cause catastrophic damage to an organization's IT platform. These products can scan various elements of data transmissions including data packet and content streams like electronic mail/attachments (What is Malware, n.d.; Henry, 2013; Laudon & Laudon, 2014). There are numerous purveyors of these products including MacAfee, Symantec and Microsoft (Security Product, 2015)

Generally, an anti-malware software suite consists of anti-spyware and virus protection elements that are based on known malware signatures and increasingly, processes that detect behavioral anomalies such as unauthorized outbound data transfers or processes that run substantially longer than warranted for the task set involved (Framework, 2014; Critical Security Controls, 2015; Security Product, 2015). Moreover, there are vendors -- ProofPoint, CISO and others, who provide Cloud-based services that perform malware scans and malware intrusion

prevention on an organization's network (usually at the network perimeter) (CISO, n.d.; Security Product, 2015)

Ideally, organizations will implement malware protections at multiple points in their network security frameworks – along the perimeter and within the various layers of their firewalled zones, as well as on network-connected end-user devices such as desk top computers, smart phones and tablets (termed end point protection). An important and sometimes overlooked protection in this area is the automatic blockage and/or scanning of portable devices that are sporadically connected to network-accessible equipment – for example, USB storage sticks digital cameras, CD/DVD drives, etc. (Critical Security Controls, 2015).

Keys to success in this area include provisioning automatic updates for new threat signatures and propagation of these updates through the network to all target devices, along with the ability to add signatures and address blocks (blacklisting) on an ad-hoc basis. Also, the software must log suspicious and anomalous events for scrutiny by administrative and security staffs (Information Technology, 2009; Framework, 2014; Critical Security Controls, 2015).

Wireless Connections

Wireless access -- from mobile devices and configurations, has become a significant network security concern. In no small measure, this is due to the fact that by their very nature, wireless technologies can access organizational networks without the need for physical connections. Left unattended then, wireless channels can become attractive vectors for cyberattacks (Critical Security Controls, 2015). In essence, by using wireless devices, access points and networks, hackers and criminals can by-pass protections geared to cover only wired data flows. The threat vectors include wireless access points near or inside premises, mobile

computing devices brought into an organization's offices and newly configured wireless local area networks (WLANS) (Framework, 2014; Critical Security Controls, 2015).

Writing for NIST, Souppaya and Scarfone (2012) note that for WLANs, organizations will need to look toward establishing separate wireless configurations for employees and guests/external partners. The latter might include consultants/service providers. This arrangement provides for asset segregation and higher levels of visibility and control of wireless access and communications. Moreover, at the device level, the same authors (2013) assert that organizations will need to ensure that connections are granted only to those mechanisms that have configurations and security profiles sanctioned by the organization, and an owner who has approval to access the network via a mobile platform for a valid business purpose. They add that organizations must impose and enforce restrictions on mobile device applications that access organizational data stores through wireless connections.

Event Logging, Monitoring, Assessment and Reporting

Once they have implemented the configuration, tiered protection and anti-malware functions discussed above, organizations must use the automated activity logs that the functions generate, with an eye toward actively learning from and responding to security events that occur on the network. This is a vital consideration. Failure to use event logs in a proactive fashion allows actual and attempted attacks to go unnoticed, and thereby exposes the organization's IT resources to damage and/or theft, notwithstanding the presence of sophisticated network security architectures (Information Technology, 2009; Framework, 2014; Critical Security Controls, 2015).

To leverage event logs, organizations will need to catalog all events on all core network-connected devices – for example, firewalls, servers, routers, switches, storage units, access

points, etc., and ensure that each produces event logs in standardized formats (same data elements, formatted in a consistent fashion) (Critical Security Controls, 2015). Ideally, the organization will be able to consolidate information from these logs into a separate centralized source that provides for sufficient unalterable storage space (write-once to prevent illicit modifications), along with archiving capabilities for aged data in the event that longitudinal analysis of log files is required (Log Management Best Practices, 2011; Critical Security Controls, 2015).

In conjunction with the event log data sources, techniques and tools associated with Security Incident and Event Management (SIEM) applications allow organizations to automatically analyze and report on events detected on the network. This includes automatic reporting on anomalies and confirmed security issues such as the creation of unauthorized services, illicit port scans, unsanctioned configurations, blocked traffic and the like (Kavanagh, Nicolett & Rochford, 2014, Framework, 2014; Critical Security Controls, 2015). Companies like McAfee, Hewlett-Packard and IBM Security market enterprise level SIEM products (Kavanagh, Nicolett & Rochford, 2014).

Connecting with the institutional dimension of the security program, organizations will need to plan for the allocation of staff time to the on-going review and assessment of reports generated from the SIEM application. Assigned staff can hone automated rules for segregating anomalies from routine events, and most importantly, generate alerts and recommend enhancements and updates to the security program based on the trajectory of threat vectors reflected in the SIEM reports (Framework, 2014; Critical Security Controls, 2015). Moreover, in cases of a damaging event or breach, the organization will need to have documented and tested response protocols in place. This, too, links with the institutional dimension of the security

program. In this area, Swift (2010) highlights the importance of standard operating procedures and the need for documented roles for security staff. Further, industry guidance points to the need for escalation procedures and communications plans -- for internal staff, customers, partners, law enforcement and general public as applicable, along with response/remediation routines (Framework, 2014; Critical Security Controls, 2015).

Scanning/Testing

To bolster the SIEM program, organizations are advised to develop programs that run automated vulnerability scans on all network-connected devices on a scheduled basis. Companies like McAfee, which are laboratory certified, provide tools that automatically scan network-connected devices and provide scores on vulnerability levels and details on identified problems (Security Content, 2014; How McAfee Scan Reports, n.d.). These reports form the basis for on-going tuning and remediation of data communications networks.

Another key process in this area is penetration testing. Here, organizations develop test scenarios that mimic known or anticipated behaviors of threats and then run scripts that test to determine whether the threats can affect targeted networked resources (Information Technology, 2009; Framework, 2014; Critical Security Controls, 2015). There are numerous software products available that can be employed to construct, run and report on penetration tests (Software Testing, 2013).

As with the event monitoring and assessment reports discussed previously, assigned staff can use reports generated by vulnerability and penetration testing tools to deliver prioritized lists of the most critical issues to designated system administrators. In turn, in accordance with the organization’s institutional support plan for security, administrators can follow up on and remediate the issues surfaced via scanning/testing (Swift, 2010).

Application Program Hardening

Software applications are vulnerable to exploitation, most especially web-based software code, and thus, these network-connected resources fall under the scope of holistic security programs. Coding mistakes are a particular concern here. For example, coders may produce programs that: do not filter out illicit inputs including threats – for example, remote procedure calls and SQL Injection; fail to block the display of error messages that give insight into network and infrastructure navigation; display user inputs and thereby lead to cross site scripting issues (injected code that permits by-passing of access controls); and display of user names (allows for experimentation with log-in credentials) (Siddharth & Pratiksha, 2010).

The SANS Institute specifies several controls in this area (Critical Security Controls, 2015). These include checking to ensure the most recent versions of third party software are installed (see Secure Configurations above), using web and application firewalls (see Tiered Network Defense above), and for in-house, custom-built applications, implementing processes within the system development life cycle that rigorously test for, identify and eliminate coding errors that lead to vulnerabilities.

Access Controls

One of the most basic functions of a security program involves granting access privileges to network-connected/general IT assets based on formal classifications of persons, devices and programs, which have verified identities and the requisite, bone-fide business needs for such access privileges. This requirement also encompasses limiting access to physical IT and network assets to authorized individuals. Organizations that fail to address access controls run higher risks of significant security failures (Information Technology, 2009; Framework, 2014; Critical Security Controls, 2015).

Organizations can employ tools such as Microsoft's Active Directory to establish least-privilege, role-based security covering all individuals, processes and devices accessing network-connected IT resources (Desmond, Richards, Allen & Lowe-Norris, 2013). In a least-privileged arrangement, assigned roles (for employees, partners, contractors, customers, constituents, etc.) are bound to vetted and approved identification codes and passwords that allow only those access rights (read and/or write) based on the minimum requirements to perform tasks approved by the organization (Gegick & Barnum, 2013). To support the least privilege access regime, organizations will need to implement: identification authentication and trust checks, including criminal background checks, to verify that individuals granted access to IT resources merit this privilege; programs that assign unique log-in identifiers; strong password protocols with forced end-user resets – for example, at thirty or sixty day intervals; and procedures that ensure the removal of access privileges from individuals who leave the organization and/or who no-longer have a valid reason or authority to retain access (Minimum Security Requirements, 2006).

To grant secure network-based access to authorized partners – for example, consultants and system vendors, and/or to remotely-located employees, organizations may implement least-privilege access rights via virtual private networks (VPN). VPNs provide for encrypted (ciphered/scrambled) connections to a network via the Internet, and therefore, are often described as secure communications tunnels (Geier, 2013).

A special consideration in this area is strict control over administrative account privileges. With administrative privileges, an end user has virtually unlimited control over network and general IT assets. Thus, the compelling need for strict controls over granting and managing these privileges is clear (Melber, 2007; Framework, 2014; Critical Security Controls, 2015). Previously-described scanning, configuration/password management and event

monitoring/reporting techniques help to pinpoint misapplication and illicit use of administrator credentials and privileges. Moreover, organizations are advised to implement policies and procedures that strictly limit grants of administrative privileges to trusted and trained individuals only (at the network, server and local device levels), who have specific, valid business needs to exercise administrative rights (Melber, 2007; Framework, 2014; Critical Security Controls, 2015).

A related activity concerning account privileges centers on monitoring and controlling account status throughout the organization. Here, to prevent illicit use of end-user accounts by unauthorized individuals (theft of accounts and impersonation of authorized users), organizations can take several basic steps including: routinely reviewing accounts and disabling those that no-longer have a valid business purpose; revoking accounts of terminated employees or disassociated contractors/partners and customers; requiring strong passwords and password resets; encrypting passwords; monitoring for unsuccessful log-in attempts; providing automated lock-outs (for example, recording incidences of three consecutive failures and locking the implicated account thereafter); employing screen locks with preset time-out's; and auditing for attempts to access de-activated accounts (Framework, 2014; Critical Security Controls, 2015). These steps can be integrated with the event monitoring and reporting regime described earlier.

Another dimension of access control centers on logical and physical separation of network-connected resources. In plain terms, it makes sense to separate mundane, non-critical assets such as general information and reference content stores from assets that house/manage critical and sensitive resources like databases that store confidential, proprietary and/or regulated information (recall here the discussion on asset classification and risk assessment) (Critical Security Controls, 2015). In a conglomerated environment, nefarious actors can gain access to

low value resources, expand the exploitation to critical assets, and then export (steal) high value information using the organization's own network. To combat this problem, organizations can cordon off high value or sensitive systems/data stores by assigning them to virtual local area network(s) (VLANS) that are protected by their own firewalls (Framework, 2014; Critical Security Controls, 2015).

The final element in access control is not technological. Rather, this element focuses on controlling physical points of access to network and general IT resources – that is, limiting access to only authorized staff, most likely staff associated with the IT function itself. Controls include the use of guards at the points of entry and egress to IT resources, implementation of employee identification badges with swipe chips and/or biometric elements that allow access to locked areas (computer rooms, wiring closets, server clusters, etc.), and positioning of video cameras covering secured areas (Protecting Your System, n.d.; Framework, 2014; Critical Security Controls, 2015).

Data Asset Protection

Data assets exist in various forms and formats – from structured databases to unstructured content like video recordings, audio files and electronic images, and they permeate the typical organizational network and IT terrains (Nemschoff, 2014). These assets are stored in multiple on-line, near-line and off-line facilities. They flow within network boundaries and across network thresholds to reach the Internet, with sources and destinations that can be anywhere on the globe (Laudon & Laudon, 2014). To protect these assets, it is necessary to inventory them (see the subsection on Asset Classification and Risk Assessment above), and then implement protective measures.

One of the most basic and effective protective measures is encryption. Encryption uses software keys to scramble data so as to make it incomprehensible to anyone who is not authorized to view it, as well as to validate the integrity of communications (proving back through hashing algorithms that original communications have not been altered). Depending upon the level of protection and the administrative mode employed, organizations may use shared keys to encrypt/decrypt messages in transit, key management infrastructures for encrypting/decrypting data in storage and/or public-private key pairs with trusted public certification authorities (Public Key Encryption) for message security (Laudon & Laudon, 2014). Overall, encryption helps to prevent cyber criminals from making use of any data they are able to intercept or otherwise misappropriate, and also protects the organization in the event of accidental data loss – for example, an end user losing a removable disk containing organizational data.

Optimally, encryption is employed while data moves through the network (data in transit), and while it is stored within the organization's storage fabrics (data at rest). An example of a strong encryption process for data at rest is the Advanced Encryption Standard (AES) (Information Technology, 2009; Beer and Holland, 2013; Framework, 2014; Critical Security Controls, 2015). For data in transit, Secure Socket Layer (SSL) and Transport Layer Security (TLS) are commonly-used methods that employ encryption, while Internet Protocol Security (IPSec) addresses secure transmissions at the IP level (Stine & Dang, 2011). Wireless standards for encryption include Wired Equivalent Privacy (WEP) and the now-preferred Wi-Fi Protected Access 2 (WPA2) (Laudon &Laudon, 2014). Finally, the Secure Shell protocol protects remote command line communications (for system administrator level instructions and the like) (Rouse, 2005).

Data loss prevention (DLP) is another important tool used for data asset protection. It employs rules-based software processes that leverage the organization's data classification scheme (see Institutional Elements section above) to track data resources tagged as sensitive and/or high value as they move within the network and across network boundaries. Here, the organization may use software to detect anomalous activities -- for example, unusually large outbound network traffic volumes, suspicious destinations and unauthorized encryption of data, to prevent/suppress illicit communications. From a procedural viewpoint, DLP programs may also encompass enforcement of rules that restrict use of removable/portable data storage devices and storage of organizational data on mobile devices (Critical Security Controls, 2015).

Back-up/recovery also bolsters the organization's data loss prevention capacities (and also connects with continuity of operations/disaster recovery as discussed below). Data travelling through the network and/or residing within the organization's storage fabrics can be damaged, corrupted or lost. For this reason, security programs must encompass back-up/recovery measures to assure continual availability of vital data resources, as well as the application software programs that operate upon the data (Elmasri & Navathe, 2011; Framework, 2014). Generally, back-up/recovery involves making copies of operational data and programs from all network-connected and stand-alone systems (full and incremental copies of data and periodic full copies of software systems -- disk-to-tape and/or disk-to-disk) on a scheduled basis, and maintenance of the back-up media in secure, remote sites (potentially including a Cloud-based service provider's facility). Back-ups are designed for use in cases where the organization needs to restore (recover) all or portions of its data/systems complement from back-up media (Elmasri & Navathe, 2011).

Continuity of Operations/Disaster Recovery (COOP/DR)

COOP relates directly to business continuity planning. It involves the use of fail-over techniques that leverage replication of mission-critical data and software systems at remote locations, along with use of redundant network/processing components and facilities, including mirror images of the organization's security platform (Laudon & Laudon, 2014).

COOP is based on the identification/prioritization of mission-critical assets, an exercise that often occurs during the inventory process described previously (see the subsection on Classification and Risk Assessment above). With COOP, in the event of a catastrophic loss of a mission critical system/network, including a loss associated with a security event, the organization is able switch over to the replicated/redundant facilities in real time, or within an acceptable timeframe as defined by management (Laudon & Laudon, 2014). Budgetary and technical capacities may limit the scope and breadth of the organization's COOP program, but if the assets involved are associated with institutional viability or public safety – for example, a stock brokerage operation or emergency management network, robust investment in fail-over facilities may be necessary.

DR is closely aligned with, and in many respects, incorporated within the business continuity paradigm. In fact, the Federal Emergency Management Administration (FEMA) points up that IT technology disaster recovery planning should occur in conjunction with planning for operational continuity, with DR being focused more directly on recovering mission critical systems and networks following a major man-made or natural catastrophe (IT Disaster, 2012). Here again, prioritization of assets is a critical consideration, and the organization must specify objectives for resuming targeted systems and networks (timeframe for recovery) and recovery point objectives for data restoration. Both of these objective sets are dependent on the

organization's information system/data back-up system described in the preceding sub-section (IT Disaster, 2012).

FEMA describes other key aspects of a DR program, including acquisition of replacement hardware, software, data and networks. The approach to acquisition depends on the recovery time objective. Tight timeframes may require pre-purchase and some level of installation of these items in an alternate site owned or leased by the organization (with or without power initially – cold versus hot site). Moreover, organizations will need escalation and communications plans to notify/activate staff in the aftermath of a disaster, and to alert the media, stakeholders and law enforcement as appropriate. Finally, organizations will need to be able to connect to an alternate network via mobile devices and/or recovery office space(s) (IT Disaster, 2012).

Conclusion

This paper explored the basic elements of a holistic security program for organizations with networked IT infrastructures and systems. It stressed the need to address both institutional and technical elements that span the entire enterprise and all areas of the IT complex. The institutional elements included the establishment of the chief technology and information security officer roles, budgeting, project management, governance, training/education, asset classification/risk assessment and auditing. The technical elements encompassed: network/infrastructure mapping; standardized/hardened configurations and application programs; scanning/testing for security threats; event monitoring, assessment and reporting; wireless protection techniques; multi-level firewalling; use of malware protection software and access controls; data asset protection; and COOP/DR. The paper presented the concept of the holistic security program in a dual context – one that highlighted both the vital importance of networked

information systems and the expansive/expanding threats to the integrity of these systems. This helped to underscore the pressing need for holistic programs.

In terms of future developments in the field, from a general perspective, it would seem reasonable to conclude that organizations will continue to experience the same dynamic that has been apparent for the past decade. In this regard, one observer used the metaphor of an immune system to characterize the dynamic – that is, network and IT security professionals, the IT industry and government will function as a collective immune system that fights off attacks and evolves new immunities in response to the continued actions of adversaries in the networked, global cyber environment (Daya, n.d.). Today, we see the dynamic being played out in the development of security mechanisms that improve upon multi-factor authentication/access regimes, enhanced mobile payment systems (for example, Apple's mobile payment technology), processes that build on the strengths of the new Internet addressing scheme (IPv6), and enterprise level security defined increasingly via centrally-controlled software security program suites (Daya, n.d.; Mathis, 2013; Industry Applauds, 2014; Beaver, K., 2014). These developments will continue to impact various levels and facets of the network and general IT infrastructures. Strong institutional leadership, governance, planning and project management will be required to leverage the developments. Hence, there will be a compelling need for holistic security programs for years to come.

References

2013 - The impact of cyber crime. (2013, November 1). *Infosec Institute*. Retrieved from http://resources.infosecinstitute.com/2013-impact-cybercrime/

Acceptable use policy template. (2009). *Standard Operating Procedure Tips*. http://www.standardoperatingproceduretemplates.com/procedure/acceptable-use-policy-template/6/

Avila, k. (n.d.). *What does a firewall do?* Retrieved from http://www.cavsi.com/questionsanswers/what-does-a-firewall-do/

Bayuk, J. (2009, June 16*). How to write an information security policy*. Retrieved form http://www.csoonline.com/article/2124114/strategic-planning-erm/how-to-write-an-information-security-policy.html?page=2

Beaver, K. (2014). *Software-defined security: The future of network security?* http://searchsecurity.techtarget.com/tip/Software-defined-security-The-future-of-network-security

Behm, R. L. (2003). *The many facets of an information security program.* SANS Institute. Retrieved from http://www.sans.org/reading-room/whitepapers/awareness/facets-information-security-program-1343

Daya, B. (n.d.). *Network security: history, importance, and future*. Retrieved from http://web.mit.edu/~bdaya/www/Network%20Security.pdf

Casey, B. (2013) *Identifying and preventing router, switch and firewall vulnerabilities*. Retrieved from http://searchsecurity.techtarget.com/tip/Identifying-and-preventing-router-switch-and-firewall-vulnerabilities

CISO cloud-web. (n.d.). *CISO*. Retrieved from http://www.CISO.com/c/en/us/products/security/cloud-web-security/index.html

Coupey, E. (2005). *Digital business: Concepts and strategy.* (2nd ed.). Upper Saddle River, NJ: Pearson, Prentice Hall.

Critical security controls – version 5. (2015). *SANS Institute.* Retrieved from https://www.sans.org/critical-security-controls/controls

DayaDesmond, B., Richards, J., Allen, R. & Lowe-Norris, A.G. (2013). *Active directory*. (5th ed.). Sebastopol, CA: O'Reilly Media, Inc.

Elmasri, R. & Navathe, S.B. (2011). Fundamentals of database systems. (6th ed.). Upper Saddle River, NJ: Pearson Education, Inc.

Fennelly, C. (2003). *IT security auditing: Best practices for conducting audits.* Retrieved from http://searchsecurity.techtarget.com/IT-security-auditing-Best-practices-for-conducting-audits

Ferro, G. (2009, August 2). *Designing enterprise DMZ and multilayer firewall clusters.* Retrieved from http://etherealmind.com/design-enterprise-dmz-firewall-clusters/

Framework for improving critical infrastructure cybersecurity. (2014, February 12). *National Institute of Standards and Technology.* Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Gegick, M. & Barnum, S. (2013, May 10). *Least privilege*. Retrieved from https://buildsecurityin.us-cert.gov/articles/knowledge/principles/least-privilege

Geier, E. (2013, March 19). How (and why) to set up a VPN today. *PCWorld.* Retrieved form http://www.pcworld.com/article/2030763/how-and-why-to-set-up-a-vpn-today.html

Grimes, R.A. (2010, March 23). Isolated security zones yield better security. *InfoWorld*. http://www.infoworld.com/article/2628540/malware/isolated-security-zones-yield-stronger-network-protection.html

Harris, S. (2006). *Key elements when building a security program*. Retrieved from http://searchsecurity.techtarget.com/tip/Key-elements-when-building-an-information-security-program

Henry, A. (2013, August 21). *The difference between antivirus and anti-malware (and which to use).* Retrieved from http://lifehacker.com/the-difference-between-antivirus-and-anti-malware-and-1176942277

Hil, A., Young, G. & D'Hoinne. (2015, April, 22). *Magic quadrant for enterprise network Firewalls.* Gartner, Inc. Retrieved from http://innetworktech.com/wp-content/uploads/2015/04/Magic-Quadrant-for-Enterprise-Network-Firewalls.pdf

How McAfee security scan reports anti-virus protection and firewall states. (n.d.) *McAfee.* Retrieved from http://service.mcafee.com/FAQDocument.aspx?id=TS100714&lc=1033&pf=1

Information technology, security techniques, network security. (2009). *ISO/IEC 27033-1:2009(E)*. Geneva, Switzerland: ISO/IEC.

Industry applauds Apple's developments in mobile pay. (2014). FSR. Retrieved from http://www.fsrmagazine.com/technology/industry-applauds-apples-developments-mobile-pay

IT compliance and regulatory challenges. (2015). *Zoho Corp.* Retrieved form https://www.manageengine.com/products/eventlog/eventlog-compliance.html

IT disaster recovery plan. (2012, October 25). *Federal Emergency Management Administration*. Retrieved from http://www.ready.gov/business/implementation/IT

Kavanagh, K.M., Nicolett, M. Rochford, O. (2014). *Magic quadrant for security information and event management*. Gartner, Inc. Retrieved from http://www.gartner.com/technology/reprints.do?id=1-1W8AO4W&ct=140627&st=sb&mkt_tok=3RkMMJWWfF9wsRolsqjJdu%2FhmjTEU5z16uwrUKCzgZd41El3fuXBP2XqjvpVQcNlMbDLRw8FHZNpywVWM8TILNUQt8BqPwzqAGM%3D

Laudon, K.C. & Laudon, J.P. (2014). *Management information systems: Managing the digital firm*. (13th ed.). New York, NY: Pearson.

Log management best practices. (2011). Alert logic, Inc. Retrieved from http://www.alertlogic.com/wp-content/uploads/2012/01/Log-Management-Best-Practices.pdf

Mathis, R. (2013, July 29). *Global multi-factor authentication market to reach $5.45 billion by 2017*. Retrieved from http://www.secureidnews.com/news-item/report-global-multi-factor-authentication-market-to-reach-5-45-billion-by-2017/#

Melber, D. (2007, January 30). *Controlling privileges of the administrator accounts.* Retrieved from http://windows security.com/articles-tutorials/authentication_and_encryption/Contolling-Priviledges-Administraotr-Accounts.html

Minimum security requirements for Federal information and information systems, FIPS Pub 200. (2006). *National Institute of Standards and Technology*. Gaithersberg, MD: NIST.

Nemschoff, M. (2014, June 28). *A quick guide to structured and unstructured data.* Retrieved from http://smartdatacollective.com/michelenemschoff/206391/quick-guide-structured-and-unstructured-data

Pironti, J.P. (2005). Key elements of an information security program. *Information Systems Control Journal (1),* pp. 1-6.

Protecting your system: Physical security. (n.d.). *National Center for Education Statistics.* Retrieved from http://nces.ed.gov/pubs98/safetech/chapter5.asp

Rouse, M. (2005). Secure shell (SSH). Retrieved from http://searchsecurity.techtarget.com/definition/Secure-Shell

Rouse, M. (2006). *Key performance indicator (KPI).* Retrieved from http://searchcrm.techtarget.com/definition/key-performance-indicator

Security content automation protocol (SCAP) validation program. (2014, January 24). *National Institute of Standards and Technology.* Retrieved from http://scap.nist.gov/validation/

Security product vendors. (2015). *Anti-Malware.Info*. Retrieved from http://www.anti-malware.info/security-product-vendors/

Siddharth, S. & Pratiksha, D. (2010, November 2). *Five common Web application vulnerabilities.* Retrieved from http://www.symantec.com/connect/articles/five-common-web-application-vulnerabilities

Software testing help. (2013). *Softwaretestinghelp.com*. Retrieved from http://www.softwaretestinghelp.com/penetration-testing-tools/

Souppaya, M. & Scarfone, K. (2012). *Guidelines for securing wireless local area networks (WLANs): Recommendations of the National Institute of Standards and Technology*. Gaithersburg, MD: National Institute of Standards and Technology.

Souppaya, M. & Scarfone, K. (2013). *Guidelines for managing the security of mobile devices in the enterprise.* Gaithersburg, MD: National Institute of Standards and Technology.

Standards for security categorization of federal information and information systems, FIPS Pub 199. (2004). *National Institute of Standards and Technology*. Gaithersberg, MD: NIST press.

Stine, K. & Dang, Q. (2011, May). Encryption basics. *Journal of AHIMA 82*(5): pp. 44-46.

System center configuration manager (SCCM). (n.d.) *Iowa State University Information Technology*. Retrieved from https://www.it.iastate.edu/services/sccm

Swift, D. (2010). *Successful SIEM and log management strategies for audit and compliance.* Bethesda, MD : The SANS Institute.

Tate, K. & Martin, P. (2010). *The project management memory jogger*. (2nd ed.). Salem, NH: Goal/QPC.

What is malware and how do we prevent it? (n.d.). *Symantec*. Retrieved from http://www.pctools.com/security-news/what-is-malware/