

Five Key Cyberspace Defense Elements

By Jac W. Shipp

Why should you care about safeguarding information on your personal, corporate, department, or agency network?

If the information happens to be your personal health or financial information this is a simple question to answer.

For public and private sector organizations, the concern may be over potential loss of proprietary information giving an advantage to the competition. It may be National Security information the loss of which may have a direct impact on our National interests.

The specter of hackers and other cyber threats has received a great deal of attention over the past year through successful attacks on Lockheed Martin, Northrop Grumman, Boeing, Sony, and others. Threats to the safety and security of our personal and organizational data abound. Given what are likely diminishing resources in our fiscally constrained environment, how should we protect ourselves?

If we cannot build a robust defense in depth around our fortress, how can we allocate our resources to dissect, examine, and mitigate the threat?

One plan certainly does not fit all in the realm of cyber security. However, some themes and issues are common across the cyber domain. What follows is a brief discussion of those commonalities with a few suggestions about how to address them and achieve a higher level of data protection. After all, safeguarding the data on our networks is one of the fundamental goals of cyber security.

The scope of our exploration will include five key elements to an effective information-safeguarding program. These elements include system and network users and administrator training and education, the mitigation of external threats, insider threats, threat responses, and situational awareness and understanding.

The authors acknowledge this does not encompass all of the potential threats to your personal or organizational data. Areas specifically not addressed include threats to the air and space links, e.g. intentional or unintentional disruption from interference or jamming, whether of our own design through ineffective frequency management or from adversaries in the form of electronic warfare; disruption in the space link, or space transport layer from sources like space weather, threat space con-

trol activities, or anti-satellite events – intentional or unintentional. We have also not addressed events that cause disruption in the physical infrastructure including cables, fiber, or the supporting power grid. This is not to suggest these are not possible, nor important, they simply fall outside the scope of this work.

To provide a common framework for our discussion on the safeguarding of data we must have a common definition for the word ‘safeguard’ itself. Throughout this work we will use the term as both a noun and a verb. As a noun, we will use the following definition: “a measure taken to protect someone or something or to prevent something undesirable: there were multiple safeguards to prevent the accidental release of a virus.” For the verb form, we will define ‘to safeguard’ as the act of “protecting from harm or damage with an appropriate measure: low interest rates offer the opportunity to safeguard their financial futures.”

User Education and Training

The first of five key areas is user and administrator training and education, particularly in the area of threat awareness. An uneducated workforce spells disaster for protected information. Ignorance of safeguarding techniques leaves room for external threats to penetrate into and escape from networks with valuable information; internal threats to expose sensitive material without challenge; and employees to unwittingly reveal corporate and other secrets.

Even the greatest workforce doubles as an entity’s greatest weakness when unaware of safeguarding techniques.

Workforce training is both the easiest and most effective means to safeguard information. Management should train every employee – not just security personnel – in safeguarding techniques because any employee can encounter a threat or become a threat themselves. The course must emphasize constant vigilance, teach information safeguarding best practices, identify example threats, train employees to identify such threats, and detail prudent threat responses. It would double as a retraining device for those who inevitably make mistakes.

Such training should occur at least every other year. Yes, everyone hates training courses, but they prove effective nonetheless. Successful courses capitalize on the difference between asking students to pay attention and capturing a student’s attention. Employees will leave an interesting

training course with a better understanding of their role in safeguarding information than they had when they arrived. If it is not interesting, courses waste time and resources.

Mitigate External Threats

The second area is mitigation of the external threat. External threats comprise 70% of all network breaches and 98% of all detected network breaches. They come in all forms including electronic phishing and network attacks to physical supply chain and facility breaches. Taking these attacks seriously enables successful defending. Components of external threat mitigation include addressing system and network vulnerabilities, data tagging and encryption, supply chain risk management, and physical security, all reinforced by an effective program of penetration testing.

In this step you must identify system and network vulnerabilities. Some solutions are obvious—add a firewall and patch existing firewalls—but hackers do not limit themselves to conventional tactics. As the Germans did with the Maginot Line in World War II, hackers circumvent firewalls.

To counter adversarial attacks, inspect inbound and outbound network traffic at the packet level. Then run penetration testing on your networks. Hire a red team to hack your network and expose your weaknesses before an adversary exposes them for you. Continue to patrol your network to prevent your defenses from stagnating and to keep adversaries on their toes.

Data Tagging and Encryption Monitoring outbound network traffic also pairs well with data tagging. Tagging every piece of information enables data tracking as data moves through the network, ensuring that only those with predetermined access privileges have information access. The system would quickly flag, stop, and report unauthorized data requests. Tagging should occur whenever a user reads, moves, edits, etc. a piece of data. Data encryption, while common, must be more uniform. Add encryption for data both at rest and in motion. Information is vulnerable when idle or in use, so do not neglect encryption at rest. Adding security layers makes hacking that much harder when stealing your data.

Supply Chain Vulnerabilities

Hardware attacks can ravage your network just as easily as electronic attacks. The entire lifecycle of network hardware and software is vulnerable while it is not in your hands including product conception, design, building, testing, shipping, installation, maintenance, and retiring. If you do not trust those handling your products, you cannot trust the products. During production—especially non-domestic—bad actors can intentionally design “flaws” into products you intend to use giving them unlimited and unmonitored network access to do anything from interrupting internal communications to exposing your most valuable assets. Adversaries might tamper with your products while installing them, during routine maintenance, or even when retiring a product. When possible, buy domestic, trusted products. Otherwise, monitor all vulnerable points as thoroughly as possible. Also consider entering a joint venture with other bodies to sponsor a trusted third party to inspect products and/or companies for you. Individual entities can rarely tackle such massive security challenges alone, but collectively their funds

(Continued on page 24)



(Continued from page 23)

can sponsor someone to tackle it for them.

For physical security establish the best possible physical security practices for your facility. Continue to update your practices as newer and better practices become available. But unless the workforce is aware of those practices, safeguarding efforts go to waste. Keep employees up to date on practices and policies, and how carrying out or neglecting these practices helps and hurts the organization respectively.

Insider Threat

The third key area is the insider threat. The term “insider threat” includes deliberate and unintentional network breaches. While external threats account for 70% of all data breaches, 48% of data breaches – including some overlap – involve insider threats. They begin with employees accidentally or intentionally exposing something due to loose network practices and policies and end with a bad actor either compromising or selling sensitive or proprietary information.

Effective insider threat miti-

gation techniques strike a careful balance between providing information only to those who need it to complete their jobs (Need-to-Know) and distributing information thoroughly (Need-to-Share) for better productivity and situation mapping. Too much of either can prove disastrous. Information distribution first and foremost keeps the workforce aware.

The more information they have, the better they understand the big picture. Waste decreases as employees gain a better understanding of where the need is, how to fill it with their skills, and how to avoid redundancies as bureaucracy falls to the wayside. Information protection is equally important. Limiting individual access to certain data and information types decreases the likelihood of security breaches and successfully ensures individual, information, and asset safety .

The goal is to protect information enough to keep it safe from insider threats while distributing it thoroughly enough to maximize workforce efficiency and support better decision making. Develop a series of standards to help your organization meet these goals. First, ensure

that those who need to know something know it, and those who do not need to will not. Then fill in the gap between the two. Give access to those who could potentially draw connections between different fields or topics and prevent those who cannot and/or should not make connections from getting access. To alleviate this process, establish rules and automate the process to determine who should receive access to what information. Important decisions should always be made by multiple people, not machines, so use the automated access process carefully.

Another aspect of insider threat mitigation is to address the issue of writable and removable media. Flash drives, CDs, DVDs, portable hard drives, and other portable electronic devices provide effective means for transporting harmful software onto and sensitive or proprietary material off of safeguarded networks. Weak network restrictions allow both intentional and unintentional harm to the network by simply plugging in such a device.

If possible, prohibit use of these devices altogether. More realistically, if you cannot, simply limit use of the devices. Require scans of all applicable devices before every use or at least periodically. Limit what information and how information may flow to and from the devices. Finally, log all packets moving to and from the devices in keeping with the data tagging schematic.

	Most Damaging	Most Likely	Overall Priority
Lack of adequate Training and Education	2	1	1
Failing to mitigate External Threats	1	3	2
Failing to Mitigate Insider Threats	3	4	3
Lack of adequate Threat Response Plans, policies, and reporting processes	4	5	5
Lack of Situational Awareness and Understanding	5	2	4

Respond Quickly

The fourth component is having a mechanism for responding to incidents and threats as soon as they are identified. When a security breach occurs, you do not have the luxury of time to figure out how to resolve the problem. Each moment you wait lets adversaries steal additional data, compromise your network further, or even jeopardize your employees' physical safety. Develop a thorough threat response plan ahead of time to minimize the effects of critical periods.

A successful response plan must enable decision makers to make informed decisions about a threat. Therefore, response plans should include the following: threat detection, reporting, analysis, and response. Establish policies covering both external and internal threat response techniques and update them periodically. This process takes a set of initial conditions, passes an accurate summary of the situation to decision makers, analyses threat information to produce viable solutions, and provides the means to create a desired outcome.

A thorough and effective reporting process feeds decision makers' situational awareness and enables situational understanding, or allows them to take appropriate actions with a complete understanding of the consequences for those actions.

Maintain Situational Awareness

The fifth and final component of safeguarding information is situational awareness and understanding. How do you turn situational awareness into situational understanding?

First, establish a baseline for your network by determining exactly what hardware and software your network contains and how the network components connect internally and externally.

Monitor the established baseline for anomalies. Report any anomalies upward to security officials and decision makers before analyzing the incoming anomaly information to determine appropriate response options. Once you have established potential response options, visually represent the network situation for decision makers. This establishes situational understanding by providing decision makers with both an understanding of the situation itself and threat mitigation options. Then select a response and execute through the proper channels.

Unless your organization rehearses these steps regularly, though, your responses will fall apart. Rehearsing works out rough spots in both policy and

procedure, trains participants to respond, and creates second-nature responding. Without rehearsals, a real threat may arise and both insufficient policies and participants who do not understand their jobs will fail to mitigate the threat. Rehearsals should coincide with penetration testing to maximize the benefits of each test.

Unfortunately, it is unlikely we can afford to address everything we have discussed above at one time. To help prioritize our efforts and resources we can apply a risk management approach. The first step is to look at our organization and ourselves from the perspective of a hacker or insider threat. What would they view as most valuable? What would potentially cause the most damage or disruption to our operations?

We can dissect our risk by what is most likely to occur, and most damaging if it does occur. In our example we have set 1=highest, 5=lowest priority/probability. Consulting the USSS report, or your own aggregated information about data loss events within your agency, department, or organization in the past will help in this process.

With this method of prioritization, we can inform the allocation of effort and resources to address all of the key areas, phased in over time, implementing a near-term, intermediate, and long-range plan of action and develop specific milestones to track our progress toward increased information security.

Any organizational data safeguarding plan should include these five key elements. We have examined five key elements that should be a part of any organizational data-safeguarding plan. Their priorities and how you implement plans, programs, and policies associated with implementing these elements must be tailored to your unique data, users, systems, and networks. Employing a risk management process can inform your prioritization process, and should be followed by the development of a detailed plan of action and milestones to support tracking. As you implement your plan, have a set of quantifiable, measurable indicators of effectiveness to support the continuous updating and improvement of your own data safeguarding plan.

Jac W. Shipp, Scitor Corporation, advises various customers on offensive and defensive cyberspace operations. He has planned, led, and supported cyberspace operations for more than 12 years, and briefed cyber issues to the Vice President of the United States, and Directors of the Central Intelligence Agency, National Security Agency, and the Director of National Intelligence.

Join the Discussion
<https://signalink.army.mil>

