SAFEGUARD YOUR MOST IMPORTANT ASSET: INFORMATION

According to McAfee®, 60,000,000 malware programs are written every year as cybercriminals continue to push the envelope.¹ Even worse, corporate and government-sponsored computer espionage is an escalating problem on an international scale, as hackers use even more sophisticated methods to bypass security ramparts. Protecting your data is as important as protecting your cash — because anything that threatens your information systems threatens your enterprise.

What if confidential information about your customers, agency members, finances or classified projects fell into the wrong hands? You could lose your competitive advantage at best or suffer significant losses at worst. A security breach that catapults your company into the headlines would not only damage your reputation and credit rating, but expose it to lawsuits and even bankruptcy.
SECURITY RISKS COME WITH A **HIGH PRICE**

Attacks and breaches of your information systems are costly, whether it’s operational losses while you identify and rectify the problem or time and money to rehabilitate your image. Add in the strict compliance requirements that are being enforced in practically every industry – along with steep fines and stiff penalties – and proactively managing risk can save your organization innumerable complications and costs.

Done right, cybersecurity proactively manages risk. It safeguards critical information assets, ensures data integrity and protects the confidentiality of information. It also gives your organization the ability to retain evidence and prosecute effectively.

**CYBERSECURITY PUTS POLICIES, PROCEDURES AND TECHNICAL MECHANISMS IN PLACE TO PROTECT, DETECT AND CORRECT PROBLEMS BEFORE THEY THREATEN YOUR NETWORK.**

**ARE YOU PREPARED?**

**DID YOU KNOW**

- Moving from legacy analog to a highly-efficient, digital IP-based network increases complexity and introduces new risks
- Information-sharing and interoperability adds even more vulnerabilities
- Compliance and regulatory mandates are evolving and often tied to grant funding
- Breaches can result in negative publicity, financial loss and political implications
- Government budgets are decreasing while requirements for improved security are increasing
Advanced computing power and anywhere connectivity are in the palm of our hands, literally. Business devices connect us to smartphones, digital two-way radio systems and location-based asset management systems that help mobile workers keep in touch with the home office. Digital cameras upload images to the cloud, gaming systems let us compete with players anywhere in the world, and smartphones turn on lights and appliances remotely.

Anywhere connectivity has changed our expectations about the way we access information at work. Telecommuting is mainstream. Mobile data is mission-essential. Twitter and Pinterest are moving from social media to business tools. Centralized network lockup has become impossible. And data is growing faster than the ability of the network to handle it – with 667 exabytes travelling over the Internet annually by 2013, according to Cisco. At the same time, employees are bringing their own devices to work and exposing enterprise networks to a new world of vulnerabilities. People are more proficient than ever with technology and more dependent on their mobile devices. Unfortunately, most are naïve about their role in securing the devices and data you rely on – and that is an enormous risk.

Hackers are targeting government networks as they go after high-value intellectual property, and increasingly their attacks originate in foreign countries. A highly specialized worm, such as the Stuxnet computer virus, is a sophisticated cyber attack tool that shut down a nuclear facility’s entire network and is now viewed as a super weapon.

MOBILITY IS CHANGING EVERYTHING, AND CHALLENGING EVERYONE

667
EXABYTES
WITH 667 EXABYTES OF DATA TRAVELLING OVER THE INTERNET ANNUALLY, DATA USAGE IS GROWING FASTER THAN THE NETWORK CAN HANDLE.
IT SPENDING INCREASES, BUT SO DO INTRUSIONS

Most organizations concentrate much of their security budget on technical solutions. Buy the box – a firewall, antivirus program or anti-malware tool – install it on the network and consider the problem solved. As more government attention is focused on information security, “buy the box” has morphed into “check the box” to ensure that all systems comply with all the latest regulations to secure the network.

How effective is this approach? Even though 37 percent of organizations surveyed are ramping up spending on information security compliance, mobile devices and data loss prevention, intrusions are rising. According to the Privacy Rights Clearinghouse, the biggest data breaches in history occurred in 2011, with 535 breaches involving 30.4 million sensitive records reported. Even more disturbing, the majority was caused by insiders within the organization.

SECURITY IS ONLY AS STRONG AS YOUR USERS

Poor practices by users can easily overcome the best-planned and most technically-savvy security system. Do your employees understand that syncing a smartphone at an office PC or using a thumbdrive to ferry work from home to office could expose your network to malware? Do they realize that the unauthorized application they installed on their desktop PC or the peer-to-peer network for large file transfers could open backdoor access to your carefully secured systems? Do they know that if a device is lost or stolen, it could compromise the most sensitive data?

While technical solutions and compliance controls are essential, they are no substitute for a knowledgeable, security-conscious user. It is why putting the right processes in place for security best practices by your employees must be a top priority. They need to know that using a device on an unsecured network opens the door to a host of security issues.
OFTEN THE GREATEST THREAT ISN’T THEM, IT’S US

Every organization defends against “them” — the hackers, spies and other malicious entities who try to breach defenses. Less obvious is the risk created by employees inside your organization performing risky behaviors (opening attachments, clicking on links, going to malicious websites), but doing so without any malicious intent. Even the best defense can be broken by insiders who fail to follow good security practices and carelessly leave the gates down.

All of “us” in an organization must understand what information assets are kept and why access to those assets may be limited. All of us need to trust that information is safe. The more critical the mission, the more important it is that our territory is successfully defended against all threats.

OPERATING ON AUTOPILOT IS UNSAFE

Trusting a “buy the box” mechanism or a “check the box” procedure without involving users is like relying on an autopilot system without an actual pilot on the plane. Artificial intelligence is no substitute for the common sense of an informed user. If your enterprise only measures success by how well you have implemented compliance controls and overlooks operational procedures and managerial policies, they are flying blind.

A successful cybersecurity solution merges all these aspects with behavioral change, at every level of the organization. This approach — named Defense in Depth by the National Security Agency (NSA) — is a strategy for multiple layers of defense across the lifecycle of the system. It considers the technology in use, the operations of the organization and the personnel involved.

Your enterprise benefits when you educate your personnel. By making employees continually aware of and trained on current vulnerabilities and best practice risk mitigation strategies, you make security defenders of them all. And with that, users become a real tool for reducing total cost of ownership (TCO) and a vital first step toward driving tighter security.

SHARING INFORMATION IS SECOND NATURE

Many of your employees have never known a world without computers and Internet access. They use high-powered mobile devices and share data every day, at every level of their lives — whether it’s online photo albums, blogs and tweets, timelines on Facebook or real-time GPS apps.

When employees have access to your intranet or databases, sharing comes naturally. When they believe your security is interfering, they often defeat those procedures, unwittingly or intentionally. Most users don’t fully grasp the risks or anticipate the vulnerabilities. And since cybersecurity is often server and desktop focused, it does not focus on protecting the mobile and portable technologies they use most.

Security experts are being challenged to keep up with the increasing threats to digital data, as hackers exploit vulnerabilities as soon as new products come to market. The rise in cloud computing is adding another layer of complexity for organizations as users share technology, rely on providers for security and open the organization to malicious attacks by hackers able to harvest confidential data or gain control over cloud services.

THE LESS THEY GET INVOLVED, THE GREATER THE THREAT

Your employees may suffer from a lack of clarity about information security. Or your organization may not have adequately defined and implemented policies, relying on compliance measures, technical mechanisms or an IT team to protect them instead. Or lack of communication may be the culprit. Many security systems are undocumented or presented as unexplained mandates which users find easy to dismiss as productivity roadblocks or territorial directives from IT.

An informal framework without clearly documented procedures can create the perception that security compliance is optional. A lack of clear management support can also create a casual attitude that favors productivity over data protection. If your decision-makers do not prioritize security, your users won’t either. In the end, the less involvement with security policy your users have, the less responsible they feel and the more risks they unwittingly take.
CYBERSECURITY IS CRITICAL AS NETWORKS CONVERGE

Whether your agency or organization uses a two-way radio, a next generation 9-1-1, an LTE or a wireless system, there are layers of complexities associated with it. Since each layer is an opportunity for someone to exploit a security control and do damage to the network, you need layers of protection to keep sensitive information safe – from patient health records to public safety data.

In this rapidly-changing landscape, where a combination of attacks is common – such as viruses, phishing and identity theft – it’s important to implement concentric rings of protection. Such a holistic approach should take into account the entire lifecycle of security protection: from security assessment to integration to managed services, such as firewall monitoring and intrusion protection, to policy development.

A common mistake in many organizations is a lack of planning. It is simply not enough to implement a security control and rest assured. You have to maintain and review controls regularly, especially since threats to the environment are continually changing. Addressing the security process upfront is pivotal for planning your budget, too.

KEY QUESTIONS TO ASK TO PROTECT YOUR NETWORK

- Do you have an established security program which is staffed and funded?
- Has your organization conducted or updated its security risk profile?
- Do you have a vulnerability management program?
- Do you have an escalation procedure for incidents?
- Are your networks or data regulated by State or Federal law?
- Do you share information with other entities or agencies?

DEFINE YOUR SECURITY OBJECTIVES, AND YOUR USERS

When it comes to cybersecurity, it is essential to define your objectives and communicate your plan clearly. Bring together a team of users and stakeholders to explore the goals, realities, options and will of your organization.

First see if the security objective is measurable, achievable and tied to your mission. Then ask who the internal experts and weak links are, and what the current user mindset is about security. Next, consider which security challenges are best met by technical mechanisms, operational changes and user awareness – and determine how budget will affect these choices. Finally, identify attitudes and conditions that need to change, resources required and the value of outside support.

Once your team has defined the cybersecurity objectives, document your decisions and commit to an ongoing process of continuous change management. Address training with messages tailored to your different network users.

Be sure to leverage the social networks in your enterprise to build consensus and support, including management. Tap into the expertise of your internal security specialists or those outside your organization.

PRESENT YOUR POLICIES AND DISCUSS POTENTIAL RISKS

When you bring your user groups together, offer them clear policies based on well-defined goals and objectives. Clearly outline the risks each procedure is intended to mitigate. Be frank and specific in describing the potential consequences of a breach.

Your people need to understand that security risks come from both internal and external sources, and from aggressive attacks and passive vulnerabilities. This is your opportunity to inoculate your organization against social engineering threats like phishing and spoofing. Everyone should come away with a clear understanding of how Internet connectivity opens your systems to threats such as cookies, mobile code, denial-of-service attacks and peer-to-peer network backdoors.
DEFINE, DOCUMENT AND DECIDE

Awareness training needs to be a continual process in your organization to affect real change in user behavior. For employees, documentation is the textbook that supports their learning and defines the technical processes and operational procedures of cybersecurity.

AT A MINIMUM, DOCUMENTATION SHOULD ADDRESS THESE MAIN QUESTIONS

**WHO SHOULD BE USING NETWORK RESOURCES?**
Does access extend to other agencies, entities, external vendors or customers?
Should some access be restricted to certain groups of insiders?

**WHAT IS THE PURPOSE AND PROCESS OF USER AUTHENTICATION?**
What makes a good password and how do you protect it?
How does your organization use virtual private networks (VPNs) and other remote authorization tools?

**WHAT EQUIPMENT CAN BE ATTACHED TO THE NETWORK?**
How is your network protected from “infected” systems?

**HOW SHOULD A POTENTIAL SECURITY BREACH BE HANDLED?**
To whom should a stolen device or lost smartphone be reported?
What is the process for securing data access when an employee is released?

BY CLEARLY OUTLINING THE ROLES AND RESPONSIBILITIES OF YOUR EMPLOYEES IN THE INFORMATION SECURITY PROCESS, GOOD DOCUMENTATION HELPS REDUCE CONFUSION AND ENHANCE PRODUCTIVITY. IT ALSO SERVES NOTICE THAT CYBERSECURITY IS A PRIORITY FOR YOUR ORGANIZATION – SUPPORTED AT THE HIGHEST ECHELON AND RESPECTED AT EVERY LEVEL.

EMPOWER YOUR EMPLOYEES TO BE DEFENDERS

User awareness is an important defensive weapon in your cybersecurity arsenal. As your people gain a fuller understanding of the risks and costs of poor security practices, they can strengthen their role in protecting your organization. Better informed users can be security allies, accepting controls and applying them more consistently. By sharing in the responsibility to protect critical information assets, your employees become even more valuable – minimizing risk, reducing exposure and lowering costs for your entire enterprise.
THINK LOCALLY, ACT HOLISTICALLY

Security attacks are increasingly stealthy, targeted and financially motivated. Today, polymorphic attacks – capable of modifying themselves with every execution – are ubiquitous. While many organizations would like to think their most sensitive data or mission critical information is inoculated, it is not immune. Threats are growing more complex and frequent and there are no silver bullets in technology spending, compliance standards or traditional perimeter defense.

As networks converge and people collaborate and share data around the world, cybersecurity solutions must address all the people, policy, process and technology aspects holistically: from defense-in-depth security assessments to how to meet compliance requirements.

No question, proper planning is a key component of a holistic approach. By detecting and containing threats early on and implementing new controls based on lessons learned from previous attacks, your organization can adopt a productive strategy for the long term.

INSULATE YOUR NETWORK AND BENEFIT

Whether you share public safety data or patient health information, operate a two-way radio network or the latest LTE network, when you build a secure infrastructure and insulate your networks with concentric rings of protection, you benefit by:

- Increasing network reliability and regulatory compliance
- Eliminating vulnerabilities and downtime costs
- Improving the performance of your business-critical systems
- Ensuring continuity of your operations and connectivity to the market
- Achieving your mission and ultimately, helping your organization thrive

SOURCES

1. McAfee Threats Report: First Quarter 2012
2. “Public safety can benefit when hackers go bad”, Urgent Communications, August 17, 2011
5. www.privacyrights.org/top-data-breach-list-2011

To find out how to manage the complexity, visit motorolaspotentials.com/services/government