WHITE PAPER:
THE CYBER RESILIENCE BLUEPRINT: A NEW PERSPECTIVE ON SECURITY

The Cyber Resilience Blueprint: A New Perspective on Security

Who should read this paper

For business leaders. In this sophisticated threat environment, traditional security tactics are failing. Symantec encourages organizations to revisit their security posture to build a more cyber resilient enterprise. Resilience is not defined by a series of checklists, but through evaluations based on the current threat environment and the acceptable risk level for the organization. This whitepaper presents best practice-based approaches recommended for minimizing cyber risk. These are arranged across five pillars and provide specific actions for each pillar to be performed by identifiable IT jobs.

Symantec

Content

Navigating Security in the Digital Workplace

Due to a powerful combination of influences, the workplace is changing at an exponential rate. In its *Nexus of Forces*, Gartner defines this phenomenon as "the convergence and mutual reinforcement of four interdependent trends: social interaction, mobility, cloud, and information" that "combine to empower individuals as they interact with each other and their information through well-designed ubiquitous technology."[1] Increasingly dependent on connectivity, we're using the web to get work done in real-time by connecting to the Internet and others' mobile devices. Both empowering and greatly disrupting, these converging trends are making business more competitive and agile—yet also more vulnerable to cyber attack—and organizations are struggling to stay abreast of the challenges they raise. In this environment, a thoughtful security strategy is essential for security-conscious organizations.

Figure 1. Agenda Overview for Nexus of Forces

Source: Gartner (January 2014)

A Thoughtful Security Strategy

Cyber risk isn't new, but the stakes grow higher every day. An incident is no longer likely to be a single event, but a sustained and persistent campaign. Most analysts, business leaders, and visionaries have arrived at the same conclusion: there is no silver bullet, no one-size-fits-all solution, and in most cases, no single approach that will offer protection from an attack. Instead of continually putting security measures in place, businesses need to identify their most important business assets and how current security measures relate to them. It's a paradigm shift that uses security intelligence to guide decisions and support agility.

Forrester presents this as the *Targeted-Attack Hierarchy of Needs*.[2] Based on Abraham Maslow's famous Hierarchy of Needs for self-actualization, the framework focuses on the core needs required for defending the IT environment against targeted attacks, laying the foundation for a resilient security strategy. The needs in order of importance are: an actual security strategy; a dedication to recruiting and retaining staff; a focus on the fundamentals; an integrated portfolio that enables orchestration; prevention; and detection and response.

1- Agenda Overview for the Nexus of Forces, 20 January 2014 G00261499
2- Forrester Research, Inc., Introducing Forrester's Targeted-Attack Hierarchy Of Needs, May 2014 Rick Holland blog: http://blogs.forrester.com/rick_holland/14-05-20-introducing_forresters_targeted_attack_hierarchy_of_needs

Governments approach cyber risk and critical infrastructure defense through education and by providing formal strategies and frameworks. There are 35 government-published cyber security strategies globally, with more being developed all the time.[3] For example, the US government is formally encouraging the private sector to create more robust cyber security strategies (Executive Order 13636), while the European Union has seventeen published strategies. Frameworks also exist in Russia, Japan, Australia, and several African nations. Some of these attempt to set a standard minimum level of security, such as the National Institute of Standards and Technology (NIST) cyber security framework enacted in 2014 in the US; ENISA guidance in the European Union[4]; and PAS 55 in the United Kingdom. The well-known ISO 27001 security standard has also been recently updated (IEC 27001:2013) to more closely align with key cyber concepts.[5]

The Five Pillars

In this sophisticated threat environment, traditional security tactics are failing. The old methods of adding another point product to the mix or waiting for IT to identify and propose technology solutions to the business side of the house is less effective than ever. No organization can simultaneously sift through alerts, track vulnerabilities, apply security policies across various systems and endpoints, and accurately assess what a mass of global threat data actually reveals in real time. To manage these competing challenges, organizations must change their security posture from a defensive stance focused on malware to a more realistic and resilient approach—a cyber resilient approach.

Cyber resilience is about managing security with a multi-layered approach that encompasses people, processes, and technology. Correlating security intelligence is important, but just as important is increasing your employees' security IQ so they can make better decisions and reduce risky behavior. This expanded scope helps to eliminate the cyber gap between IT and business, requiring the two sides of the house to proactively align and present a united front against threat and incursion.

As threats morph and organizational needs evolve, cyber resilience is by definition about continual refinement. The process can be best thought of as a framework with five pillars: prepare/identify, protect, detect, respond, and recover. Using this framework, you can evaluate each pillar of your organization's cyber security strategy. For example looking at the pillar for prepare/identify, vulnerability assessments can expose weaknesses that exist in an organization's security posture. By evaluating the risk posed by each weakness and addressing the weaknesses that are most critical, you should be able to improve your preparedness for an attack. With each scheduled cycle of assessments, the security strategy is honed, and since every organization has unique systems and different security needs, the results of each series of assessments is evaluated based on the current threat environment and the acceptable risk level for the organization, rather than a relatively generic series of checklists.

For each of these pillars, best practice-based approaches are recommended for minimizing cyber risk, with each requiring specific actions to be performed by identifiable IT jobs.

3- ENISA http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world
4- http://www.enisa.europa.eu/publications/articles/standards-for-cyber-security
5- ISO27001 Update: http://en.wikipedia.org/wiki/ISO/IEC_27001:2013

Pillar 1: Prepare/Identify

To successfully face and overcome an attack, you must thoroughly understand your company's security and risk posture. Begin by painstakingly identifying the organization's vital information. Conduct an infrastructure and information assessment that includes all known security vulnerabilities. Establish a baseline and compare the results to those of your peers. Spotting and addressing the most urgent issues first will make your organization a less appealing target for attackers.

You'll need true business leadership, not just guidance. Real engagement from business and data owners during this phase is crucial. Together, rate information assets in terms of value to the business and prioritize what to protect. Ask, where is the data located? Who is using it? What is its value? How is it currently protected? Is it vulnerable? If so, what makes it so? This exercise also encourages greater awareness among employees regarding what can happen when they put data at risk. It helps to align business and IT in terms of cyber risk and management, while spurring culture change in employee behavior.

Specifically, focus on:

- Improving visibility and understanding your information and systems, through asset and network discovery and mapping;
- Understanding your cyber risk posture through assessments and simulations;
- Identifying and remediating vulnerabilities in your IT organization, including your supply chain, where many cyber criminals seed attacks;
- Mapping assets to vendor relationships;
- Building awareness of the external threat landscape and understanding how to recognize if you are being targeted through comprehensive global threat intelligence, correlation, and analysis capabilities;
- Making users cyber-aware through regular and on-going education on best practices and risky behavior; and
- Ensuring appropriate backup and recovery strategies are in place.

Regular training is key. As part of preparation, make personnel aware of existing cyber security policies and processes, and help them understand the business importance of those policies and processes. Individuals who aren't security savvy or not necessarily aware of the value of certain information are vulnerable to exploitation or making costly mistakes. All employees must understand appropriate handling of the organization's sensitive information, as well as what constitutes employee IP theft.

Once an organization has adopted a policy, created an awareness program, and established access controls, it must implement detection strategies and response plans. A variety of solutions are available to assist in the development of these plans, including threat intelligence services and data discovery tools. Threat intelligence plays a vital role in helping organizations prepare for existing and emerging threats.

Security intelligence gives organizations a greater understanding of the entire threat landscape, including threat perpetrators and trends. Scrutinizing their own internal infrastructure and considering the potential impacts that certain threats can have on their organization allows security managers to proactively predict threats and exploits. As a result, threat intelligence services enable security leaders to better protect and secure their environment and manage risk.

Pillar 2: Protect

Once you have a good handle on what's out there, where it lives, its level of sensitivity, how vulnerable it is, and your risk tolerance, you can begin to take the necessary steps to protect it. The second pillar is all about developing and implementing safeguards for critical infrastructure and services in order to limit or contain the impact of an attack.

Protecting your organization's infrastructure and data from malicious attack to the best of your ability is the goal. While no amount of time, money, or effort on your part can guarantee success, your job is to minimize the chance of a breach succeeding, and if it does, to be able to react quickly to reduce damage.

The infrastructure and information assessment you performed should have revealed any gaps in your existing defenses. Now, ask yourself, how well maintained and up-to-date are your existing prevention solutions? Are your defenses prepared to protect against the latest advanced threats or innovative exploits? Are you relying on disjointed point products? Are you taking an integrated approach to protection that gives you effective situational awareness and the ability to better respond to cyber risks? Do you have policies and automated enforcement in place to minimize human factor or process-related breaches? How about a feedback loop to improve outcomes?

In particular, focus on:
• Protecting your website and online users from cyber threats;
• Securing business-critical systems from cyber threats (your data center is typically the best place to start);
• Protecting the organization's endpoints and gateways from targeted attacks and advanced threats;
• Protecting your mobile workforce and customers; and
• Protecting and governing information assets over their lifecycle, including protecting from data loss or illegal access—look into encryption or using a data vault.

All three areas—people, processes, and technology—are important to the protection pillar. You must have the necessary technology in place to safeguard your critical infrastructure and assets. The technology solutions you employ must also offer protection for the increasingly mobile workforce. Safeguarding mobile access to the network and data is becoming more and more important as employees' ability to access sensitive corporate information increases. In addition, the technology must be integrated to provide the necessary intelligence that will allow for quick detection of an attack.

Managing people and processes is key. A recent Ponemon Institute study found that 35 percent of the root causes for data breaches involved human factors, such as negligent employees or contractors. The same report attributed 29 percent of breaches to system glitches, which includes IT and business process failures. Breaches related to human factors or process failures are often driven by a lack of appreciation by employees for cyber security from both the business and the IT sides of the organization. Inappropriate use, storage, or distribution of the organization's sensitive information and a lax approach toward operational and business policies are often at the root of human error.

In addition to education and awareness, organizations must monitor and enforce policy adherence. Not only does policy enforcement and monitoring improve an organization's risk posture, but it also conveys to the entire workforce the importance the organization places on its confidential information and intellectual property. A lack of policy enforcement and monitoring creates a cultural attitude with the opposite effect—if IT doesn't value and protect digital information, why should the employees?

Pillar 3: Detect

The Detect pillar focuses on developing and implementing the appropriate activities to rapidly identify an attack, assess the systems that may be affected, and ensure a timely response. In addition, this stage is concerned with continuing to monitor the network for other attack indicators related to that attack and making sure the safeguards you had in place were effective. A critical downside of an organization spending so much time and effort trying to protect itself from attacks is that the entity often fails to prepare for what to do when an attack succeeds.

One of the most significant consequences of this lack of preparation is that it cripples the organization's ability to effectively respond to the breach. As response time, and time to resolution increase, cyber criminals have more time to exploit and damage the business. With the total cost per data breach incident in the US now at $5.4 million on average, this is no small problem.[6] Damages not only include the cost of remediating the breach, but also penalties for non-compliance, loss of reputation, and/or loss of customers. Of course, if the organization lacks the necessary solutions to detect the breach in the first place, the cyber criminal can wreak havoc indefinitely. According to the 2014 Verizon Data Breach Investigations Report, 85 percent of point-of-sale intrusions took weeks to discover, and 43 percent of web application attacks took months to discover.

When a breach occurs, the only way to proactively and effectively minimize its damage is to have the necessary detection and response policies, processes, and technologies in place. While many organizations might already have detection and response strategies, they must regularly evaluate if they're adequate and determine if they can contain and remediate breaches faster. Big data and associated analytic tools coupled with the emergence of cloud, mobile, and social computing offer opportunities to process and analyze structured and unstructured cyber security-relevant data to help with this process.

Think about how to monitor internal security events and correlate them to external threats, and how to make sure the data is available to quickly determine when or whether you have been breached. Monitoring the potentially hundreds of endpoints, logins, and data access attempts on a busy network is no simple task. When you combine that with attempting to maintain awareness of the global threat landscape, it's impossible. This is where a managed security service can be helpful. Managed security offerings can range from security monitoring and prioritization to advanced threat protection and incident response management, and can help to build a resilient security strategy that allows you to quickly prepare, protect, and respond to complex cyber attacks.

The cyber resilient organization creates a proactive IT department with visibility across the entire environment, one with deep, data-level integrations that yield insight, and that constantly evolve and respond as attackers become more advanced. By correlating security intelligence, IT can quickly detect and remediate a potential issue before it spreads, resulting in reduced damage and cost.

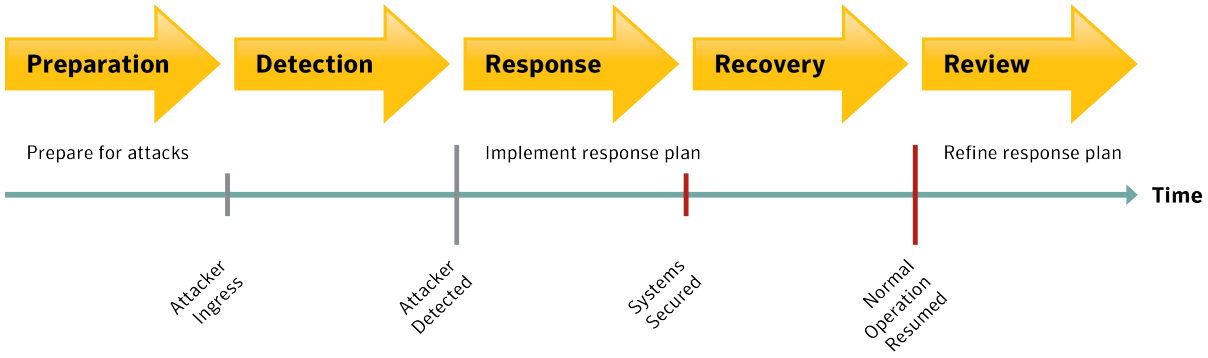
Pillar 4: Respond

The Respond pillar provides guidance on the types of activities that can accelerate time to remediation and contain the impact of the attack once it's detected. For the detection process to have any value, there must be a timely response. While there are many solutions and services available to help, much of what is needed in terms of response involves people and processes internal to the organization.

Organizations need a response plan that clearly tells people what to do when an incident occurs. A Computer Security Incident Response Team (CSIRT) should be established, with specific roles and responsibilities identified. These roles should be assigned to competent members of the organization. A team leader/manager should be appointed and assigned the responsibility of declaring an incident, coordinating the activities of the CSIRT, and communicating status reports to upper management.

Having a pre-defined action plan that is understood by everyone helps you coordinate your response efforts in a more timely and effective manner than having no plan at all. The CSIRT should be written and ratified by appropriate levels of management. It should also clearly prioritize different types of events and require a level of notification and/or response suitable for the level of event/threat.

6-



A response plan allows you to quickly determine the extent of the risk to the environment and respond. For the quickest response, automating the remediation steps is ideal, in addition to trial runs where employees practice implementing policies and procedures. In creating your plan, focus on:

- Managing risk by measuring and tracking your cyber resilience, including how well systems were protected during an attack (is there infection, or was the attack repelled?);
- Creating a plan—outline how you intend to respond to cyber incidents;
- Determining how response processes and procedures will be maintained and tested;
- Coordinating communications response activities, and understanding how analysis and mitigation activities will be performed; and
- Devising a system whereby lessons learned are incorporated into future response activities.

It can be difficult to remediate an attack. Organizations are effectively and in some cases literally held ransom when an attacker gains control of their systems. In March of 2014, the online project management tool Basecamp was hit with a distributed denial-of-service (DDoS) attack. Until the company paid a ransom, the attackers flooded the website with traffic so that legitimate users couldn't access it. In cases like this, incident response services can help organizations implement a clearly defined incident response plan to assist with recovery.

Pillar 5: Recover

The final pillar that needs to be addressed—critical to any resilient security strategy—is recovery. This stage involves developing and implementing the appropriate systems and plans to restore any data and services that may have been impacted during a cyber attack. As much as we prepare and protect our organizations, we may not be able to avoid certain types of attacks. Even if you respond quickly to a cyber breach, an attack may have consequences. No matter the outcome, organizations must be able to restore their people, processes, and systems as quickly as possible. An effective recovery depends on a clear and thorough recovery plan.

Many organizations already have business continuity and disaster recovery plans in place, with elements such as backup and recovery, cloud storage, off-site archives, redundant and geographically separated data centers, and other business continuity measures. However, these plans often fail to cover essential recovery best practices and scenarios.

For example, while most organizations perform regular backups, very few actually know what they're backing up. It's important to understand how much of the information being backed up is genuinely important to the business. If a disaster occurs, what information and systems does the business need restored first to return to normal operations? Organizations must ensure their recovery plans answer these questions.

Redundant data centers are important, but keep in mind logistical and geographic considerations that may affect failover ability. Data centers in close proximity to one another, for example, won't help if a major catastrophe hits an entire city or region. Aside from geographic considerations, what happens if an emergency wipes out communication with the data centers?

While many organizations do address these possibilities in their recovery plans, most focus on recovering from business disruptions caused by system failures and natural disasters. Many don't fully cover what to do in case of a serious cyber catastrophe.

If a massive cyber breach occurs, organizations need a plan of action for getting back to normal operations. There are many stories of organizations with comprehensive, traditional business continuity plans and regular recovery and data center failover drills that were woefully unprepared when they were actually hit with an enterprise-wide cyber attack.

Think about how a cyber breach would affect your systems, people, and processes. What will be needed if your employee's smartphones or tablets are compromised? If an aggressive malware attack renders a significant number of the hard drives in your organization's laptops unusable? How quickly can you rebuild new hard drives? Are there processes in place to provision new systems quickly for essential employees if needed? Think through all the ways a cyber attack may impact your organization. What processes and procedures are needed to recover from them?

Essentially, you must ensure your critical systems are available during an incident, and decide how you will restore other systems and data afterwards. As with response plans, recovery plans need to be re-evaluated and updated regularly to meet all of the risk-related aspects of a disaster that an organization might face.

Achieving Cyber Resilience

The impacts of a major cyber attack can be devastating to any organization. Unfortunately, no silver bullet exists to prevent attacks, and breaches will occur in spite of an organization's best efforts at preparation and protection. Many customers lack the sophistication and expertise they need to address these new, more advanced threats. To minimize the potential devastation of a cyber attack, you must change the way you think about security. Think in terms of not eliminating cyber risk but of creating cyber resilience.

To create cyber resilience, organizations must begin by changing the conversation about cyber risk. It's crucial to align IT and the business and encourage regular, productive discussions to identify the benefits and risks associated with a cyber resilient strategy. Find and use a common language. IT security must accept that the business will be tempted to take risks in order to succeed and must empower the business to make informed decisions on how they manage cyber risk.

Senior management must take a more active role in establishing and supervising a cyber security program. In a cyber resilient organization, senior management makes the decisions and is ultimately responsible for compliance. As a result, these managers must be educated about the choices their company faces and take responsibility for addressing the risks.

Ultimately, IT must move from a policing mindset to one that promotes an integrated, comprehensive cyber strategy powered by people, processes, and technology. By changing the culture around digital information and nurturing an appreciation for a strategy that encompasses preparation, prevention, detection, response, and recovery, organizations will gain true cyber resilience and the ability to respond and recover quickly from an attack.

Contact your Symantec account representative or reseller partner today to discuss how you can start building cyber resilience into your security strategy. Get more information about cyber resilience and stay informed at the Symantec cyber resilience microsite. go.symantec.com/cyber-resilience.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company operating one of the largest global data-intelligence networks, has provided leading security, backup, and availability solutions for where vital information is stored, accessed, and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2013, it recorded revenues of $6.9 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com