GuidePoint SECURITY

WHITE PAPER

The CXO's Challenge: Tackling Secure Digital Transformation

In an era marked by cybersecurity skill shortages and rising cybercrime, the responsibility shouldered by security leaders requires a keen understanding of a rapidly changing technology environment, as well as the myriad of risks associated with digital transformation business initiatives. In 2019, companies are exposed to increasing, opposing and evolving forces. But where to begin to find a balance between a finite budget and escalating need? How do security leaders identify and address the weakest links and the most significant vulnerabilities? What's the road map to a security posture that meets your specific requirements for data protection and privacy, yet enables the business to adapt to the evolving technology landscape?

Nearly

60%

of Cybersecurity Workforce respondents say their companies are at moderate or extreme risk of cybersecurity attacks due to the [cybersecurity labor] shortage.[1]

This paper provides four best practices for security leaders to:

1) Calculate cybersecurity investment
2) Prepare for an effective risk assessment
3) Develop criteria for selecting a cybersecurity partner
4) Embrace a modern approach for secure integration of products and services

Plus, the key questions a CISO should ask before purchasing security technologies.

1) (ISC)2 Cybersecurity Workforce Study, 2018 https://www.isc2.org/Research/Workforce-Study#

1) Calculating the cybersecurity investment for digital transformation

Digitalization continues to restructure business models, speed innovation and revenue, and amplify customer value. It is an evolution that is as necessary to the survival of organizations as agriculture to civilization. Yet, with new opportunities for competitive advantage come modern-day threats to company and consumer data: an increasing amount of known and unknown devices connecting to the network, frontline applications that expand the attack surface, and technologies from multiple vendors deployed by staff who often lack expertise and/or for holistic integration to maximize the value of the investment. Often, the budget for cybersecurity falls short of the business need.

Digital transformation requires the CISO to cultivate a more fundamental role with business leaders to enable automation and orchestration using data analytics. However, confidence in digital innovation begins with confidence in security. Awareness of (or first-hand experience with) cybercrime has made the ROI of security solutions and services more apparent. More than ever before, security is not an afterthought: it is being considered as integral to the larger business objective. When customers demand secure access to an application, for example, or business leaders require more consumer data (and therefore more protection), the security investment is as vital as the application itself. When the formula for investment isn't clear, some enterprises establish cybersecurity budgets in proportion to:

- Total IT budget
- Number of users
- Business metrics (revenue, cash flow and ROI)
- Value of digital assets, or
- Annualized loss expectancy

One well-known formula for calculating the cybersecurity investment factors the costs of risk exposure and risk mitigated over the cost of security services and solutions. However, in a market flooded with security products, services and claims, it's important to remember that more investment doesn't necessarily translate into better protection.

$$\frac{\text{Risk exposure + risk mitigated}}{\text{Cost of cybersecurity services/solution}}$$

Cybersecurity should be viewed as a holistic strategy in which business needs and evolving risks are understood, and where it is built-in rather than bolted-on. Consideration of cybersecurity solutions should include analysis of how the solution is best implemented, integrated and fully operationalized before purchase. Moreover, to increase the relevancy and effectiveness of cybersecurity investments, the purchase should take into account the value of assets via data discovery and classification and provide protections that deliver the highest ROI.

When organizations lack the time or expertise to conduct data discovery or fully vet new technologies, best-in-class cybersecurity service and solution integrators can support these efforts by performing a holistic assessment of existing cybersecurity measures and architecture. In addition, service and solution integrators will work to:

- Understand the business, industry context and risk profile
- Deliver customized assessments to address unique governance challenges and data privacy requirements
- Identify gaps and vulnerabilities in the digital ecosystem
- Advise the organization on how to align its objectives, technical requirements and information- security priorities with its in-house capacity

The good news for security leaders is cybersecurity budgets are growing: According to Gartner, worldwide spending on IT security will jump 8.7 percent in 2019 to $124 billion while general IT spending is expected to grow by only 3.2 percent.[2]

2) Prepping for a risk assessment

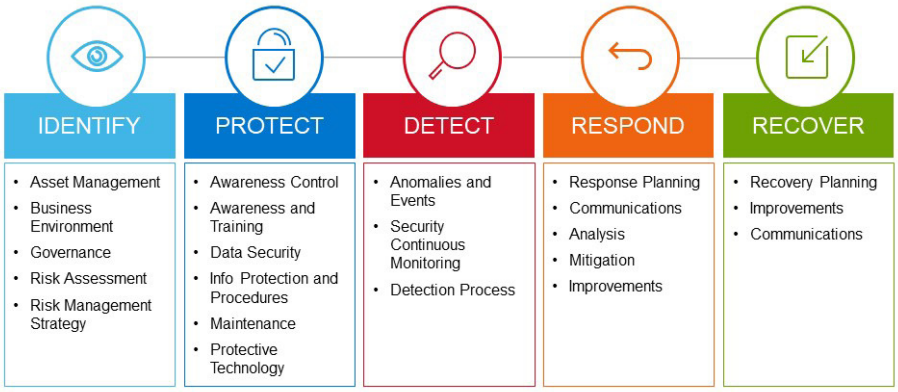
Several organizations have defined frameworks for managing cybersecurity risk. The National Institute of Standards and Technology (NIST), a unit of the U.S. Commerce Department, published a framework for improving critical infrastructure cybersecurity that has been widely adopted in the private sector. With standards, guidelines and best practices, the NIST framework helps organizations develop a current and target profile and define steps to achieve the target profile. The most common representation of the NIST framework includes five functions representing the pillars of a holistic cybersecurity program.

The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 is a data security standard with a widely accepted framework for keeping information assets secure. ISO 27001 methodology is based on a Plan-Do-Check-Act cycle, which builds the information security management system (ISMS) that maintains and improves the whole program. With constant measurement, review, audit, corrective actions and improvements, this cyclic system avoids deterioration. Achieving ISO 270001 certification demonstrates that an organization has designed and implemented a comprehensive ISMS that meets the highest standards.

2) https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

NIST, ISO and other frameworks are designed to manage risk and propose safeguards when cybersecurity risks are detected. Before technologies are selected, implemented and integrated into existing environments, the value of risk to the assets being protected must first be assessed. A gap analysis determines the variances between requirements set forth in regulations, guidelines and best practice standards and the organization's current security program. However, many organizations lack the time, resources and knowledge to conduct this critical analysis.

NIST Cybersecurity Framework Overview



Ground rules for a risk assessment

If the goal of the organization is to achieve the best security posture at the best cost, the first order of business is an assessment. A risk assessment is the starting point for risk mitigation. It should be customized to meet the specific needs of the organization—with purpose, scope, assumptions, constraints, information sources, and a risk model (or analytic approach) defined before the assessment begins. Security leaders must consider the following questions prior to assessment in order to communicate security priorities:

1. What is the 3 to 5 year business strategy across all lines of business?
2. What security tools are currently in use and how are they integrated?
3. What data is sensitive? Where is sensitive data stored? Who has access to it?
4. How many users and devices are in the network(s)?
5. What is the cadence of the security refresh cycle?
6. Is the security program built on a framework, such as NIST or ISO?
7. What are the company's information security policies and procedures? Are they aligned with its current environment?
8. How is the status of the information security program communicated to key stakeholders?
9. Does the organization have a vendor risk management program?

In addition, security leaders should examine staffing levels. The cybersecurity workforce gap is now the number one concern of survey respondents, according to the Cybersecurity Workforce Study.[3]

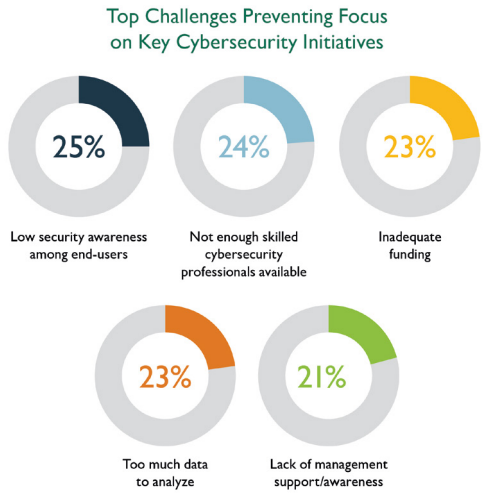
3) Ibid

3) Key criteria for selecting a cybersecurity partner

In the Cybersecurity Workforce Study, nearly sixty percent of survey respondents say their companies are at moderate or extreme risk of cybersecurity attacks due to the [cybersecurity labor] shortage. It is estimated that by 2021 there will be 3.5 million open positions for cybersecurity personnel.

The top eight areas of needed expertise include:

- Security awareness
- Risk assessment, analysis and management
- Security administration
- Network monitoring
- Incident investigation and response
- Intrusion detection
- Cloud computing security
- Security engineering



These statistics make a strong case for utilizing a security solutions and services partner that aggregates these forms of expertise to address and manage cybersecurity.

Key criteria for selecting a partner

1. **Be specific.** Choose a specialist over a generalist. Companies offering a portfolio of IT services and products do not attract cybersecurity professionals at the top of their profession. The work of cybersecurity professionals is more valued when it is core to the business and does not compete internally for resources and funding—a condition that marginalizes cybersecurity contributions and impedes growth.

2. **It's a journey, not a destination.** The best partners look at security as a process and offer more than just IT expertise. It's well known that reducing the risk of a cyberattack is not simply a technical challenge. It requires a multi-disciplinary team with broad and deep understanding of the operational environment—and the ability to respond quickly with trustworthy advice specific to your business needs—rather than a cookie cutter approach.

3. **It's who you know.** A worthy partner (against) crime, brings a strong network across the security industry and offers access to the latest intelligence and best practices. They will have familiarity with the tactics, techniques and procedures used to target your organization or industry.

4. **Been there. Done that.** Third-party advisors support in-house strategy and vision by reducing the need for a time-consuming, reactive approach to threats in favor of an informed, proactive approach to protection and mitigation. For example, in the federal arena, a security partner with personnel who have "lived the mission" will include individuals who have served in cybersecurity, counterintelligence, counter terrorism and counterproliferation missions across DoD, civilian agencies and the IC.

5. **Paid their dues.** Seek a security and solutions integrator that has earned advanced technical certifications and partner program levels. These awards recognize achievement of and continuous training in enterprise-class skill sets.

The following designations and certifications demonstrate the most-respected and prestigious credentials in the information security industry:

- **SANS Cyber Guardian:** The pinnacle of information security certifications designed for elite teams of security professionals in the armed forces, Depart of Defense or other governmental agencies. Fewer than 50 professionals worldwide have achieved this status.
- **SANS GIAC Security Expert (GSE):** The most prestigious credential in the IT security industry with fewer than 250 individuals achieving it since 2003. Its performance based, hands-on training demonstrates that a candidate has mastered the wide variety of skills required by top security consultants and individual practitioners.
- **Offensive Security Certified Expert (OSCE):** is an ethical hacking certification that teaches penetration testing methodologies and the use of the tools included with the Kali Linux distribution.
- **Certified Information Systems Security Professional (CISSP®):** is a globally recognized standard of achievement that confirms knowledge in the field of information security.

4) A modern approach to comprehensive integration of products and services

Perhaps the greatest benefit of a long-term partnership with a security solutions and services integrator is the partner's familiarity with client infrastructure, applications and teams. The strongest relationships are focused on outcomes—to the benefit of the client—to enable elimination of redundant and risky technologies, to minimize security gaps and vulnerabilities, to streamline processes and provide rapid response and recovery in an environment where continuing escalation is the name of the game. A service-based relationship increases the bandwidth of in-house engineers—who are already running thin— and brings new learning and capabilities to in-house security staff.

As businesses undergo digital transformation and the threat landscape expands and permutates, the once purely technical role of the security leader has been elevated. Whereas information and security were once part of the business, in many cases today, they **are** the business—making the modern CISO role a vital and strategic component of company management and continuity.

Today, the CISO's purview is vast. He or she is responsible for:

- Strategic planning and budgeting
- Cyber risk and intelligence
- Data loss and fraud prevention
- Security architecture
- Identity and access management
- Security program management
- Investigations and forensics
- Governance

Security should be built-in, not bolted-on. Before a new app, cloud deployment or a security solution is acquired, a CISO should ask these questions:

1. Have we assessed the value and sensitivity of affected data?
2. Do we have the right staff to support this technology (either in-house or outsourced)?
3. Do we have a plan to simplify/ consolidate the tech stack? Will this solution play well with existing technology in my ecosystem?
4. What problems will this solution help us solve?

The modern CISO understands business needs and what is necessary for digital transformation. They understand where the data is located, its sensitivity and how to protect it—including what regulators require. He or she drives security education of the workforce, and importantly, understands the unwieldiness of implementing a cybersecurity strategy single-handedly.

By seeking a partner with a diverse portfolio of security solutions, services and experts, security leaders improve their ability to holistically integrate products and processes to more securely and efficiently operate in the digital realm.

Conclusion:

The security landscape is evolving rapidly—making it impossible to embrace the status quo. The emergence of apps, cloud migration, IoT and proliferating threats require rethinking security strategy on a regular basis. Augmenting company resources with a cybersecurity partner helps organizations identify risks early, deploy best-fit solutions and resources more efficiently, and protect their environments and data more effectively.

The right cybersecurity solutions and services partner aligns overall business objectives to minimize cyber risk by:

- Determining what's needed to plan and configure for secure enterprise growth
- Developing partnerships with the security leadership team to expand their capabilities
- Bringing a depth of understanding to support holistic technology integration
- Advising on processes and technologies that are suitable for company size, structure and the industry in which they operate
- Staying apprised of the evolving threat landscape and emerging technologies
- Bringing new skill sets to in-house engineers

GuidePoint SECURITY

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132

CORPOV-WP-CXO-CHALLENGE-072019-02