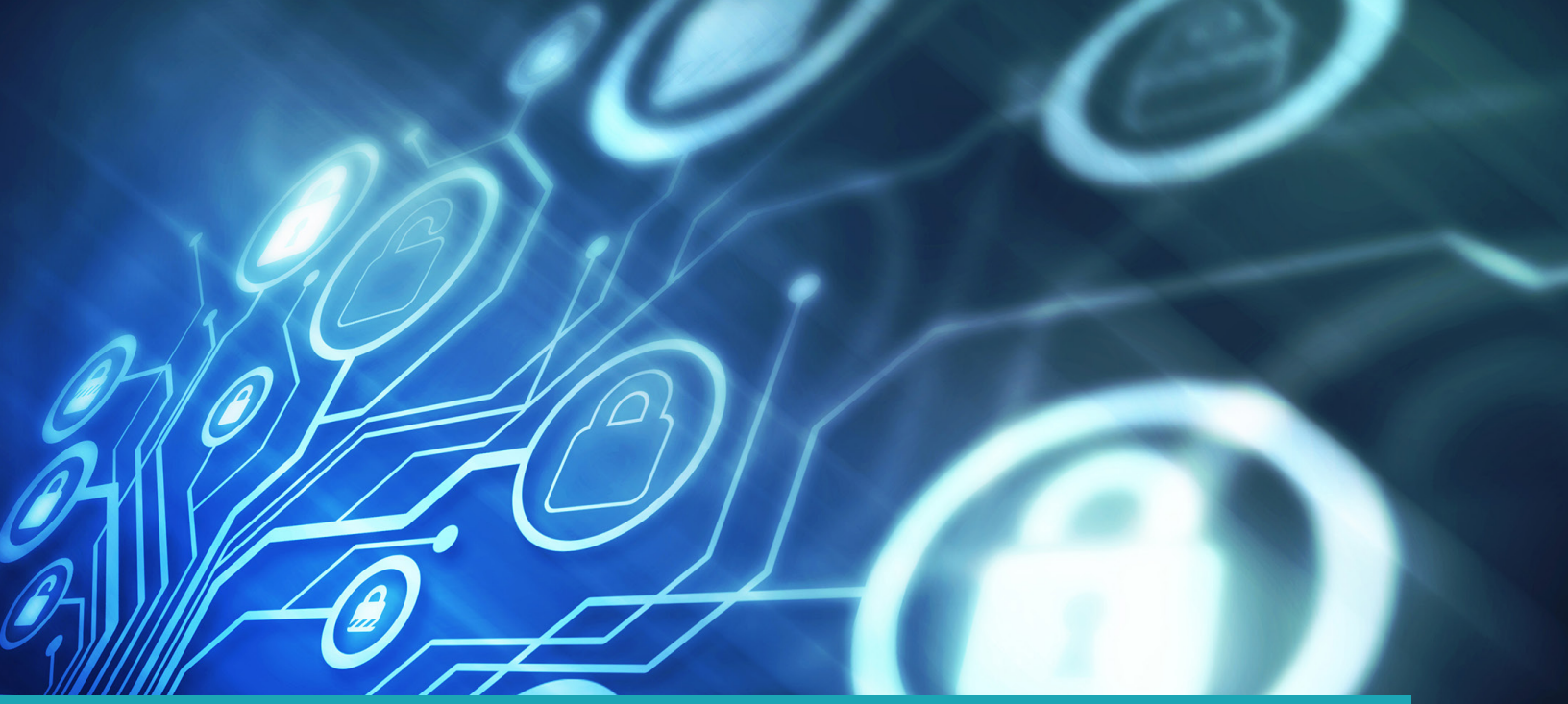

BUILDING A SECURE FOUNDATION TO REDUCE CYBER RISK

As the modern attack surface rapidly expands, companies must get the basics right. Here are best practices for building a secure foundation.

Each time a data security breach hits the news, there are reactionary questions around what could have been done to avoid the problem. Yet often—as in the case of the recent NSA breach—these incidents occur because organizations commonly overlook basic security practices.

Unfortunately, this situation will likely get worse as the attack surface expands, resulting in escalated cyber exposure. For example, the IT landscape is quickly becoming more complicated in the multi-cloud era as companies increase spending in all forms of cloud: hybrid, public, and private. Complexity will also increase with expanded use of containerized environments, and the convergence of operational technology and information technology networks. Add to the mix the rise of sophisticated and varied security threats and it paints a bleak picture as organizations attempt to stay ahead of their attackers in an increasingly digital world.

Companies must understand and effectively adopt foundational security practices that support security frameworks and compliance requirements. This paper will examine the benefits and challenges associated with the adoption of a security framework, and present best practices for achieving a strong security foundation.

The need for a security framework

Many companies are struggling with cybersecurity. In fact, 52% of respondents to the Dimensional Research survey "Trends in Cybersecurity Frameworks and Foundational Controls" said their cybersecurity program either has major gaps or weaknesses, or many minor ones.

tenable™

IDG STRATEGIC MARKETING SERVICES

Security frameworks (see Framework Providers box) present organizations with a standard, well-accepted approach to addressing cybersecurity. The overarching principle is to adopt a set of controls in a logical order, with subsequent controls building on previous ones. If the order is not followed, you won't get the expected results, and successive controls will be less effective and less efficient. Two examples of security frameworks where the controls build are the NIST Cybersecurity Framework with its Identify, Protect, Detect, Respond and Recover functions, and the CIS Controls.

The benefits of having basic controls within a security framework are clear. According to a Dimensional Research study, organizations using a security framework for less than a year accrue a range of benefits, including:

- improved security operations

- reduced frequency of security incidents

- achieved compliance with contractual obligations

The long-term (3+ years) benefits are even more significant: continued compliance; the effectiveness of security operations; and the ability to effectively present the organization's state of security to senior leadership.

Of course, there are challenges in the adoption of security frameworks. In the Dimensional Research survey, nearly all companies (94%) reported some obstacles—whether organizational or technical—while trying to implement a security framework. Two that stand out:

- a lack of trained staff

- budget

Other challenges include: a lack of integration among tools; lack of appropriate tools to audit the effectiveness of controls; and a lack of appropriate tools to automate controls.

"A framework facilitates an understanding of risk within the business, and those understandings allow you to identify the most critical projects that you must have." — Russ Kirby, CreditSafe CISO

FRAMEWORK PROVIDERS

Center for Internet Security (CIS):
https://www.cisecurity.org/controls/

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 27001 and 27002 standards:
https://www.iso.org/isoiec-27001-information-security.html

National Institute of Standards & Technology (NIST):
https://www.nist.gov/cybersecurity-framework

Payment Card Industry (PCI):
https://www.pcisecuritystandards.org/pci_security/standards_overview

The role of a secure foundation solution

After selecting the appropriate framework for your company, the key to successful adoption rests with the organization's ability to implement the various controls. With today's expanding attack surface, it is essential to be able to identify and protect all IT assets, no matter where they exist.

Consider, for instance, if your organization elects to embrace the CIS Controls as its security framework. CIS provides organizations with a prioritized set of actions (controls) designed to protect the enterprise and its data from known cyberattack vectors. Composed of 20 controls, the first five are foundational for effective cyber hygiene:

1. Inventory of authorized and unauthorized devices
2. Inventory of authorized and unauthorized software
3. Secure configurations of hardware and software
4. Continuous vulnerability assessment and remediation
5. Controlled use of administrative privileges

These first five controls eliminate the vast majority of cyber exposures. In analyzing breaches, the Australian Signals Directorate found that if organizations had implemented basic foundational controls, 85% of intrusion techniques would have been mitigated.

The foundational controls in security frameworks help organizations build a base for reuse and flexibility that can streamline compliance with the other frameworks and regulations.

Beyond this, however, it is necessary to secure the entire organization against pervasive threats that often escalate in parallel with cyber exposure. Here is where it is critical to automate the operation, assessment, and reporting of these controls to prevent threats. Unfortunately, on average, organizations automate only 45% of foundational cyber security controls.

While some administrative controls such as training may not require automation, the technical controls monitoring IT environments should gather and process data continuously to effectively gauge conformance. These activities result in far too much data to handle manually, and few organizations have the human resources necessary to fully dedicate to this task. This issue will only get worse: The non-profit information security advocacy group ISACA predicts there will be a global shortage of 2 million cyber security professionals by 2019.

To ensure basic foundational security, organizations should embrace a foundational security solution that addresses the breadth of the IT environment. Such a solution must integrate with a multitude of tools and technologies to enhance discovery, assessment, and analysis.

Having a foundational security solution can help overcome the challenges associated with implementing the controls in part through automation. One of the primary challenges is that successful and sustainable adoptions are often a multiyear project— meaning people need a logical way to get started and most importantly, prioritize each step. This is why it's important to have a solid strategy.

Strategic approach to building a solid foundation

There are several best practices companies should take, which will ease the selection and implementation of a security framework.

Start simple.

There are significant benefits to embracing a methodical approach. No organization can apply all controls at once. Incremental implementation addresses the most important aspects first, and then builds. For instance, start with a subset of a business system such as a CRM application, where critical customer data often resides. A single starting point allows the security team to build an internal set of lessons learned that it can then apply to other business systems. This also establishes a foundation to apply subsequent controls.

Although the goal is to have all these controls operating concurrently, the reality is that it takes time to fully implement them. Many companies use the prioritization found in CIS to put together an implementation plan. And for good reason. The 20 CIS controls are the result of industry practitioners working together to develop and maintain a best practices-based approach to security. Adhering to the process with its sequential steps helps organizations build on success.

Understand that ad-hoc tools alone do not yield success.

Relying solely on the latest tools may provide a false sense of security, causing teams to inadvertently create gaps or security weaknesses. This is especially true when there is a lack of integration among technologies. For this reason, the initial focus should be selecting a framework that will serve as a road map, and then implementing its controls as a means to establish security fundamentals.

Failing to embrace a framework hampers the organization's ability to grasp the big security picture. Proven templates help organizations avoid glaring gaps, and security frameworks guide the implementation of controls.

It is also worth noting that when using a framework, security teams have a vehicle to talk risk and budget with executive management. According to CreditSafe CISO Russ Kirby: "A framework facilitates an understanding of risk within the business, and those understandings allow you to identify the most critical projects that you must have."

Additionally, the foundational controls in security frameworks help organizations build a base for reuse and flexibility that can streamline compliance with the other frameworks and regulations.

"A great wealth of knowledge is created around a framework. Standardized tools that help with compliance and drive automation enable you to complete your programs more quickly. If you have a framework, your job is easier because when you create a map, you realize that 70 to 90% of the controls are common between various requirements."

— Kalpesh Doshi, CISO, Capgemini

Seek expertise to assure successful implementation. Companies need more than just a technology vendor to build a secure foundation. The right solution partner should be able to offer best practices and procedures that help define and document repeatable processes.

A strategic partner also provides experts with a deep understanding of security controls, cyber risks, and the modern attack surface who can provide mentorship and guidance—especially when IT staffs are stretched thin. Likewise, access to an ecosystem of technology partners allows for easy integration across the IT environment.

In a world where cyber attacks are a growing problem, and IT complexity continues to intensify, no organization can afford to ignore the importance of embracing, deploying, and maintaining a security platform capable of evolving in step with the ever-changing threat landscape. Security frameworks represent a proven pathway to a secure environment.

To learn more about how enterprises around the world are benefiting from security frameworks, read the eBook, "**The Economic, Strategic and Operational Benefits of Security Framework Adoption**."

Tenable™, Inc. is the Cyber Exposure company. More than 23,000 organizations of all sizes around the globe rely on Tenable to manage and measure their modern attack surface to accurately understand and reduce cyber risk. As the creator of Nessus®, Tenable built its platform from the ground up to deeply understand assets, networks and vulnerabilities, extending this knowledge and expertise into Tenable.io™ to deliver the world's first platform to provide live visibility into any asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, large government agencies and mid-sized organizations across the private and public sectors. For more information, visit: **www.tenable.com**

tenable™

IDG STRATEGIC MARKETING SERVICES