RISK-BASED SECURITY GUIDE

NNT SECURITY THROUGH SYSTEM INTEGRITY | CIS Center for Internet Security®

Transforming from Compliance to Risk-Based Security

The Complete Guide

Table of Contents

Current State of Cybersecurity

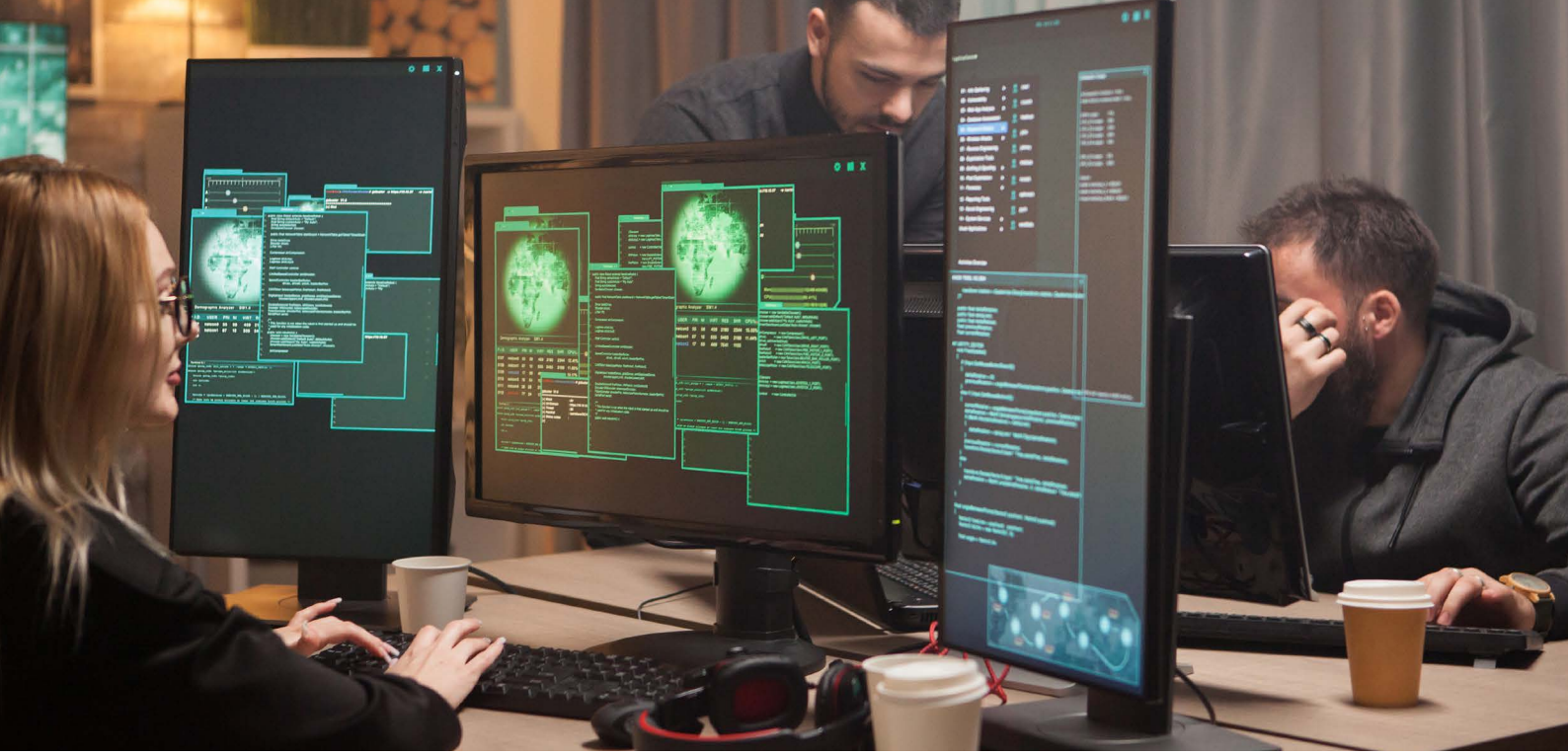
As technology evolves, the potential for cybersecurity risks amplifies greatly, and so do techniques employed by unscrupulous cyber criminals, leaving organizations grappling with securing their organization against data breaches, ransomware attacks, DDoS attacks, phishing and a variety of other cybersecurity challenges.

Many organizations fall into the trap of navigating cybersecurity challenges without adequate preparedness - this refers to the lack of a clear and comprehensive security strategy and limited visibility into the organization's maturity in responding to cybersecurity threats and incidents. These inefficiencies are further compounded by security vulnerabilities created by:

- Complex IT environments riddled with legacy systems
- Complex regulatory requirements
- Substantial cybersecurity talent gaps
- Insufficient capabilities and preparation to effectively respond to a breach
- Potential insider threats
- Lack of alignment on strategic security initiatives and compliance maturity
- The global demand to adopt digital transformation initiatives

Unsurprisingly, the 2020 Thales Data Threat Report – Global Edition with research and analysis by IDC reveals that the more digitally transformed an organization is, the more likely it is to be breached.

Furthermore, according to the report, 45% of organizations leveraging the top two digital transformation categories, Software-as-a-Service (SaaS) and social media, experienced a breach in the past year.



Relying on a compliance-based approach to solve security challenges

Compliance, while closely related and heavily supported by security, is practiced to satisfy external requirements and facilitate business operations. It also helps identify critical gaps in your existing Information Security program that may have otherwise been invisible outside of a compliance audit.

Drawbacks of adopting a reactive, check-the-box compliance mindset

It's important to note that compliance, at its very core, is only a set of legal and/or regulatory requirements that are either industry specific or industry wide. Businesses that tend to adopt a "check-the-box" approach to meet these compliance obligations, end up with a dangerous, false sense of assurance that simply because they are compliant, they are also secure.

Let's delve further into why this approach is misguided and can backfire when dealing with pervasive cybersecurity threats.

While meeting compliance obligations is mandatory, it only serves to protect narrow areas of confidential information determined as such by regulatory bodies, typically referred to as 'in-scope'

It is not designed to strengthen your organization's security posture nor does it take a comprehensive view of the various types of cybersecurity risks your organization can be subject to, particularly in the ever-evolving threat landscape within which we all live

Due to lack of an in-depth, comprehensive view, a compliance mindset results in unnecessary spending while taking away investment from areas that may be better attended to, based on actual risk rather that the boxes on a compliance requirements sheet

A compliance mindset is limited to only checking a box and meeting obligations, but fails to consider the intricacies and uniqueness of individual organizations, thereby reducing their efficiency in dealing with cyber risks and leaving them highly vulnerable to attacks

Gartner's research document 'Compliance Is No Longer a Primary Driver for IT Risk and Security' further establishes the importance of this approach, *"Compliance should be treated as a domain of risk within a formal risk management program and should not be allowed to dominate decision making."*

The solution is to move from compliance-based to risk-based security

The basis of adopting a risk-based security approach is for business leaders, mainly CISOs, to proactively address even the most nuanced threats to their business.

It does not diminish the importance of compliance, but takes into account that a truly effective Information Security (IS) program ensures both compliance and security go hand-in-hand. Building a robust approach to achieving and maintaining security and compliance requires that you allow both these areas to complement each other.

Security helps build a firm foundation for your organization, while robust compliance practices build on that foundation to ensure that the business is protected from every angle. Emphasizing equally on both these areas will empower businesses to not only meet regulations set forth by the government and standards for its markets, but also demonstrate that it goes above and beyond in fulfilling its commitment to cybersecurity, thereby fostering long-term trust with customers and the wider market.

What is risk-based security and why it is more effective than a compliance-focused approach

Adopting a risk-based approach helps you achieve three vital objectives:

Better planning of investments:

Once you assign reducing risk as the primary goal, you are able to direct your investments towards the implementation of strategies or purchasing of solutions that will increase the effectiveness of your cybersecurity program

Leveraging a framework approach to guide implementation:

Lofty risk-reduction targets can be refined down to effective program implementation, including both strategic and practical controls, adopted across the organization from C-level executives to frontline workforce.

Build controls to preemptively strike the most dangerous threats:

A risk-based approach shifts the organization's focus from building controls across all functions to building appropriate controls for the most critical security vulnerabilities, those that target your business's most vital functions.

How organizations can adopt smarter, more holistic management of cyber-risk

We recommend the following actions to help align your organization towards a risk-based approach and introduce appropriate complementary measures to minimize enterprise risk.

Align your cybersecurity strategy with business outcomes

As organizations look to integrate newer technologies across various areas of their businesses in order to achieve faster growth and innovation, it's important to align digital strategies with your security approach. This helps guide your investments in new tools, technologies and business processes, and fosters collaboration with other business leaders (both technical and non-technical) in the organization.

Security controls and requirements should be integrated at the beginning of each project or development cycle to best reduce risk. A security professional should be assigned to each new project from inception, to ensure that security requirements and controls are validated or designed into the project. The first step in ensuring appropriate positioning of your security program is to perform an exhaustive risk assessment - identify risks, assess time and effort expended in addressing them, as well as what disruptions would be caused if they were left unprotected. A framework that takes into account both risks and their impact in an enterprise-wide business context, helps you fully embed cybersecurity in the mindset of the organization, thereby enabling increased awareness and more effective management of cybersecurity.

Cultivate a risk-aware work culture

Once the C-Level Executives and board has decided on the foundation for fostering a risk aware culture, it is important this knowledge is shared with the other members of the organization. This can include issuing written documentation of the policies and procedure, communicating directly with individuals to further elucidate these policies, and offering ongoing educational and awareness programs to ensure this is made a priority.

Identify and address vulnerabilities

A vulnerability is a weakness which can be exploited by a cyber criminal to breach security, and obtain unauthorized access to install malware, steal or modify data or destroy critical assets. It is imperative that you survey and assess security vulnerabilities and risks across your entire organization, among people, processes, and technology - both those that are internal to your enterprise as well as those outsourced to/from third parties. These vulnerabilities can include software, network and physical vulnerabilities and can be identified by conducting penetration testing or using automated vulnerability scanning tools.

Ensure that both technical and non-technical decision makers are equipped with the data required to make informed business decisions that address the risk their strategies may introduce to your business.

Identify security threats faced by modern businesses

Analyze and account for threat actors, their capabilities and the security vulnerabilities they seek to exploit. This includes monitoring groups or individuals whose goals may fit closely with your organization's assets - these can be financial gains or a sinister attack on your reputation, thereby causing long-term opportunity loss.

Identifying threat actors and the tactics or methods they may use to attack your enterprise security posture is critical to building the right foundation for your security strategy. Organizations that keep themselves extensively informed about the surrounding threat landscape are able to minimize risk, implement relevant controls and preemptively counter attacks with appropriate preventative security measures.

CIS RAM (Center for Internet Security Risk Assessment Method)

CIS RAM helps to address the questions of "how much security is enough" and what constitutes "due care" and "reasonableness." It is a powerful tool to guide the prioritization and implementation of the Center for Internet Security's (CIS) Controls, and to complement their technical credibility with a sound business risk decision process. It is also designed to be consistent with more formal security frameworks and their associated risk assessment methods.

CIS RAM lets organizations of varying security maturity navigate the balance between implementing security controls, risks, and organizational needs. The core of CIS RAM is the Duty of Care Risk Analysis (DoCRA) methodology that allows organizations to weigh the risks of not implementing the controls and its potential burden on the organization.

CIS RAM is available as a free download from https://learn.cisecurity.org/cis-ram, where you can also find more information.

- CIS RAM contains detailed instructions, examples, exercises and background.
- CIS RAM Express contains a quick guide to designing and conducting a risk assessment.
- The CIS RAM Workbook contains templates and examples that are referred to in CIS RAM.

Measure and report on the performance of your risk-based approach

As you shift from a compliance checklist-oriented approach to an integrated risk-based approach, it is vital to change how you measure success. This requires performing an ongoing analysis of how effective it has been in reducing enterprise risk. Measuring it against appropriate indicators, risk appetite, key cyberrisk indicators (KRIs), and key performance indicators (KPIs) are critical in introducing improvements to your approach. If it's not measured, it's not managed.

NNT recommends the CIS Controls as an essential ‘go to’ resource for any organization looking to strengthen their data security and compliance systems

The CIS Controls are a prescriptive, prioritized, and simplified set of cybersecurity best practices and defensive actions that can help support compliance in a multi-framework era.

> *“The majority of cyber breaches occur when basic security controls have not been implemented and managed. Implementation Group 1 of the CIS Controls are effective against the Top 5 attacks as described by the Verizon Data Breach Report.”* – Curtis Dukes, Executive Vice President of Security Best Practices & Automation Group at CIS.

The CIS Controls are leveraged by organizations around the world to provide specific guidance and a clear pathway to achieve the goals and objectives described by multiple legal, regulatory, and policy frameworks. In the latest version, V7.1, the CIS Controls are prioritized in Implementation Groups (IGs). Separating the CIS Controls into IGs make their application across multiple frameworks easier.

Implementing all of the CIS Controls is the definition of an effective cybersecurity program. Effectively implementing IG 1 represents basic cyber hygiene for any organization. The CIS Controls map to most major compliance frameworks, including the NIST Cybersecurity Framework, NIST 800-53, ISO 27000 series and regulations such as PCI DSS, HIPAA, NERC CIP, and FISMA.

How collaborating with NNT can help you achieve seamless continuous compliance & robust security

NNT combines an IT management methodology and best practices from both security and IT service management, resulting in a holistic, comprehensive and prescriptive approach to solving security. This strategy is what NNT calls SecureOps™.

NNT enables, supports and secures IT digital transformation for businesses across various industries. We offer products and services that are built around security best practices, the CIS Controls, and are geared towards solving real-world problems.

Instead of using separate tools to achieve different compliances, you can use integrated solutions that align with the CIS Controls to help you navigate compliance requirements and deliver a risk-based security program far more efficiently.

How NNT and security best practices from the CIS help to support risk-based security

NNT assesses your current security governance, guides you in creating a risk-based security strategy, and offers ongoing comprehensive support in your journey.

A risk-based approach to cybersecurity includes identification of cyber threats and vulnerabilities, estimation of the likelihood of events, and establishment of standards of care. Duty of care risk analysis (DoCRA) seeks the balance between harm that may come to others, and the burden of safeguards to protect them. It assures the business that security priorities are aligned with what matters.

The CIS Controls are mapped to MITRE ATT&CK's knowledge base of adversary tactics and techniques based on real-world observations. The mapping of CIS Controls to known attack vectors helps organizations understand what they are helping to prevent when they implement each safeguard, or Sub-Control.

Additionally, implementing the CIS Controls can help demonstrate duty of care and whether implementation of a control was considered "reasonable" in preventing a security breach. Legislation in the U.S. indicates implementing the CIS Controls demonstrates duty of care.

For example, Ohio's Data Protection Act names the CIS Controls as a framework that Ohio businesses can implement to receive legal safe harbor from litigation resulting from a data breach. Nevada's S.B. 302 requires data collectors to maintain records containing personal information of state residents to implement "reasonable security measures" to protect the records, and named the CIS Controls as the state's first minimum standard of information security.

NNT
SECURITY THROUGH SYSTEM INTEGRITY

CIS Center for Internet Security®

Schedule a Free Consultation:

US - (844) 898-8362,

UK - 01582 287310

info@nntws.com

www.newnettechnologies.com

US - 518-266-3460

www.cisecurity.org