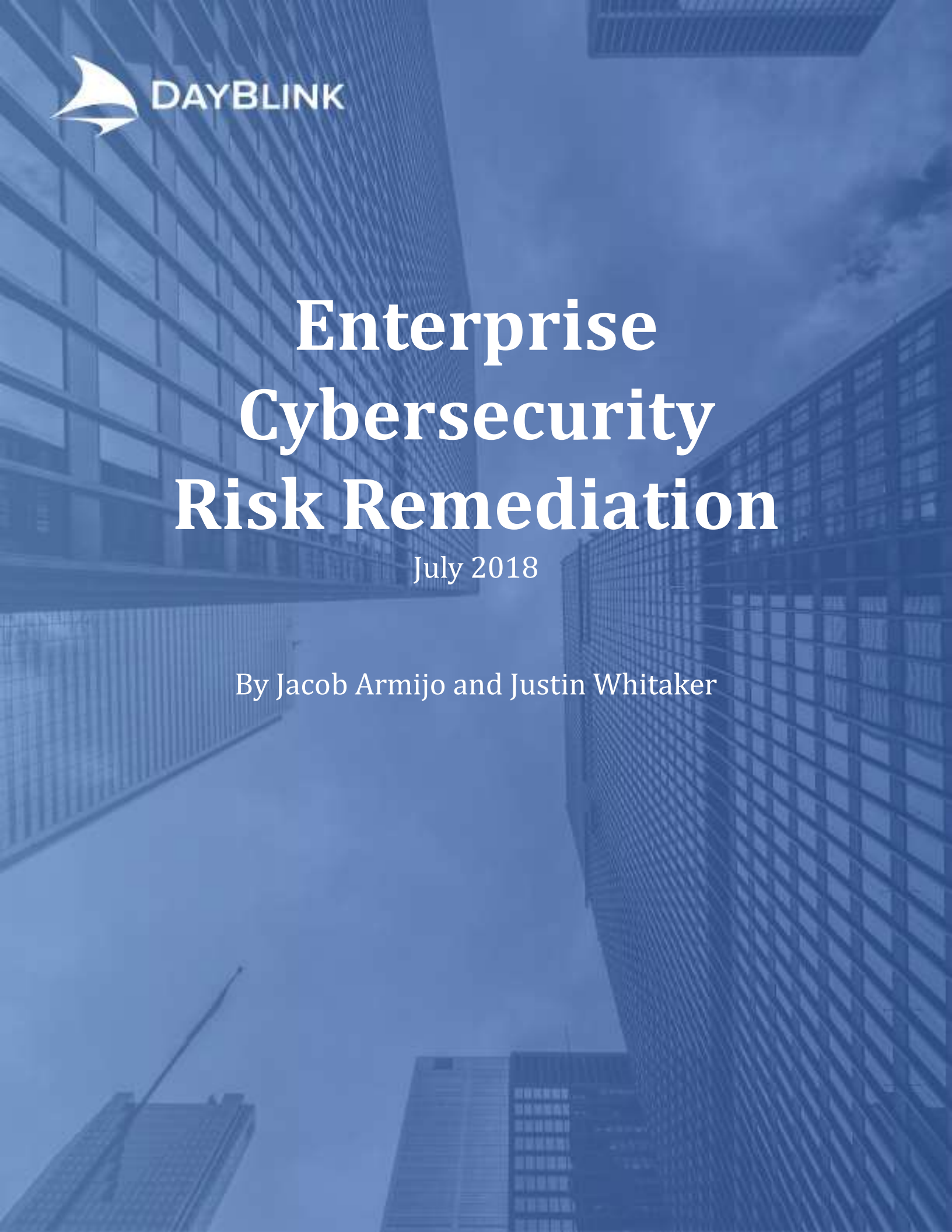


Enterprise Cybersecurity Risk Remediation

July 2018

By Jacob Armijo and Justin Whitaker

As large organizations grow and mature, they will often find themselves facing similar challenges in proactive risk management and remediation – particularly in the realm of cybersecurity. While information technology companies have historically been the most aware of cybersecurity risk, they remain exposed to threats to their products, services, network, systems, and data. These organizations recognize the pressing need to be both informed of cybersecurity risk exposure, advancements by attackers, and be prepared to defend and mitigate these risks.

Organizations encounter cybersecurity risks from a myriad of threat vectors, ranging from common vulnerabilities to environment-specific threats. As the volume and complexity of cyber threats increases exponentially, many organizations have had to address these challenges in a more ad-hoc manner in an attempt to keep pace with the threats. Historically, cybersecurity was not a top priority for many, usually taking a backseat to ensuring products and services have a rich feature set with a focus on speed to market. While this will always compete for priority, with more and more companies suffering from headline-worthy attacks, company leadership and boards are increasingly devoting more of their annual IT budget to cybersecurity spending [1]. While investment is on the rise, the challenges to securing systems and safeguarding data are only getting more complicated.

This document explores several of the operational challenges that organizations face in establishing and maintaining a sustainable cybersecurity risk remediation program. These challenges include:

- Defining risk baselines
- Establishing a method of risk prioritization
- Optimizing risk remediation processes
- Developing reliable and useful metrics

Organizations should consider both long term opportunities for improvement in each of these challenge areas, as well as immediate steps to quickly improve risk remediation practices across the entire cyber threat landscape.

Defining Risk Baselines

Challenge: Getting Lost in the Massive World of Cybersecurity

Large enterprises - such as banks and financial institutions, energy and utilities, communications, etc. are all aware that they need to have a risk mitigation strategy in place. Interestingly, they all share common challenges in understanding the baseline against which they should be evaluating risk. Using a variety of risk assessments to ensure that security policies and standards are tested and validated can often be a complex task for many information technology organizations; however, even having the correct policies, standards, and procedures in the first place can be even more of a challenge.
Figure 1, above, illustrates the scope of dozens (or even hundreds) of security procedures within the scope of a defined number of policies that your organization may be considering. All of these documents may be benchmarks against which you can evaluate risk and should be drafted with regard to your organization's risk tolerance and needs.

DayBlink Procedure Library

The figure above illustrates the scope of dozens (or even hundreds) of security procedures within the scope of a defined number of policies that your organization may be considering. All of these documents may be benchmarks against which you can evaluate risk and should be drafted with regard to your organization's risk tolerance and needs.

Opportunity: Make Molehills out of Mountains

Typical Industry Definitions of a Policy Hierarchy:

Policy: Highest level; the "Must do" items of the security world. These should typically be designed as more strategic rather than tactical. Policies should rarely change once established.

Standards: May be one or many standards per policy. Every standard is mandatory and contains a defined list of controls which are quantifiable requirements (e.g. password must be 8 characters in length)

Guidelines: Security best practices. These are not required "rules of the road", but should be included in awareness and training campaigns as ways for teams to further incorporate security into their development and practices.

Procedures: The How-to tactical documents drafted for teams to execute against standards and guidelines.

- **Define a set hierarchy of "rules"-** Clear boundaries between policies, standards, and security controls can streamline the risk assessment process and help with executive reporting or transparency into risk assessment findings. Your Organization may have a high-level Risk Remediation Policy, but assessments of all types should likely consider more granular controls to create actionable risk findings.

- **Configure security assessment tools appropriately** - Especially for automated technologies like vulnerability scanners and configuration checkers, ensuring proper rules and settings is an essential step for your information security teams. Stock configuration may evaluate systems or assets against all possible checks, without regard to your organization's risk tolerance and defined security standards. Creating a manageable backlog of risk findings is key to a successful remediation

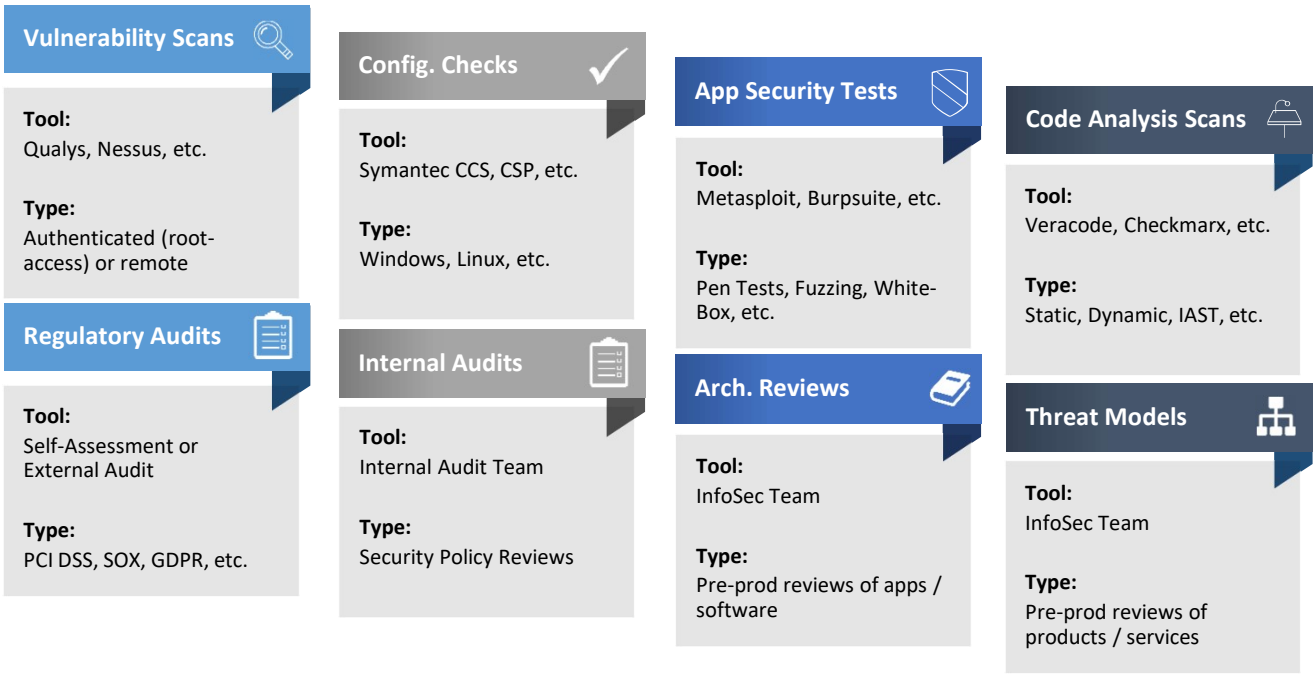
- **Re-assess and Re-evaluate** – Risk tolerance may change over time. New attack vectors or external threats can alter your strategy and your information security team should have the opportunity to re-evaluate their security standards and controls and how those will affect risk assessments / findings. An adaptive strategy to risk management is a long-term strategy to risk management.

Risk Prioritization

Challenge: Where to Start?

Remediation of even minor cybersecurity risks is likely not an immaterial cost for your information security team [2] and companies of all levels of security maturity have an opportunity to drive time & cost efficiency in their remediation process. For IT professionals and cybersecurity teams at all organizations, the methods of identifying these numerous cybersecurity risks are growing in number as part of a maturing enterprise risk remediation program (as illustrated in the figure below).

Sample Methods of Risk Identification



For example, a vulnerability scanning tool may identify thousands of known CVEs (without counting any vulnerabilities that may not even be CVE tagged) across your enterprises' IP space with time and money needed to remediate all of those individual items. However, vulnerabilities are just one example of risks faced by financial and Information technology organizations. Regulatory reviews, security assessments, or internal audit teams may identify numerous other cybersecurity risks or process weaknesses that need to be fixed as part of a cybersecurity remediation management program. Starting from item #1 and working downwards can be a limiting factor to the success of your remediation teams.

Opportunity: Focus, Focus, Focus

- **At first, simplify the risk scoring process** – The holy grail of risk prioritization, dollar-value based risk evaluation, can be a long-term ambition, but the complexity and guesswork needed to assign a dollar value to each risk can limit the initial effectiveness of simple risk frameworks. Starting with an industry standard like CVSS v2 is a key building block of a risk remediation process.

- **Layer in company-specific factors** – While CVSS Base scores are a great starting point, as your security team matures, adding in environmental scoring (CVSS or self-developed) aides your teams in pinpointing the most pressing risks to your specific organization. Although this adds a layer of complexity, your IT teams know their assets best and will have a true picture of mitigating factors or other defenses in place that a base scoring framework will not take into account.

- **Develop a framework that allows for wins –** If everything for your risk management team is a priority, then nothing ends up actually being a high priority. Any risk scoring framework should be developed such that teams have the opportunity to be successful. For example, prioritizing only “Critical” or “Urgent” (CVSS terminology) can allow for a full completion during a set time period (e.g. monthly scans) since there should be fewer of these items across a full distribution of identified vulnerabilities.

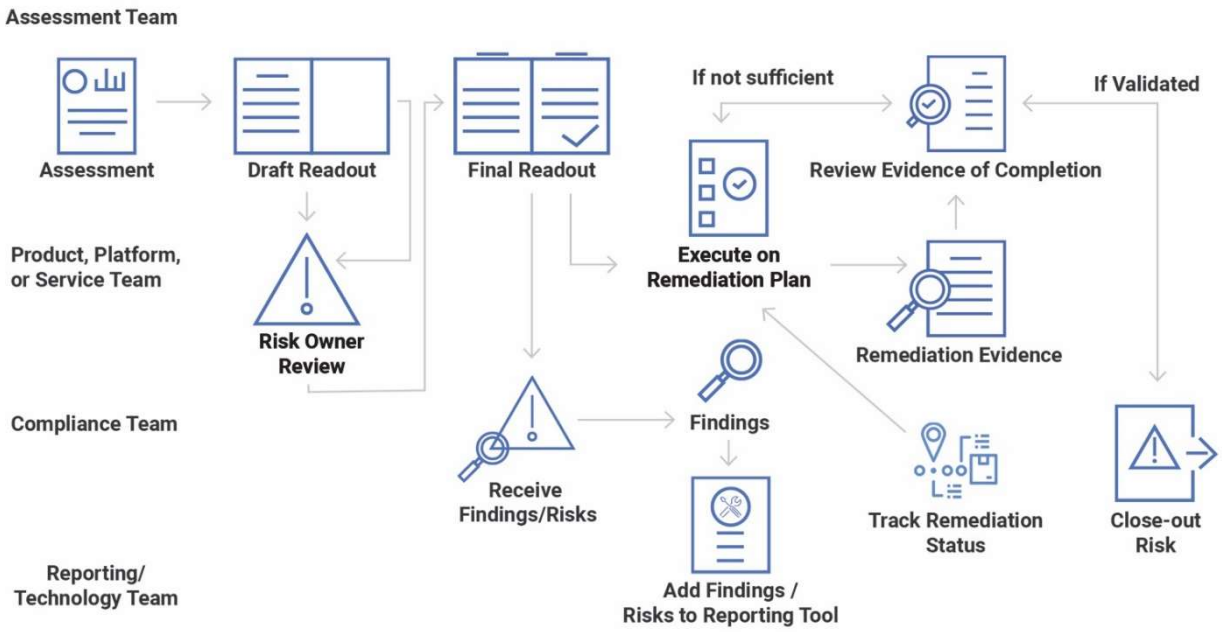
Risk Remediation Processes

Challenge: The Remediation Process Has Design Flaws Too

Risks are often identified as design bugs in applications, products, or systems; it turns out the risk remediation process also contains inherent “bugs” that can be roadblocks to a successful cybersecurity risk management program.

Risk management will vary generally from organization to organization, especially in terms of organization and governance, but as seen in the graphic below, the process can typically be generalized as Findings -> Remediation -> Completion. However, it is often the bugs in the intricacies within each of those steps that can be inherently flawed, but not without opportunity to improve.

Generalized Risk Remediation Workflow Diagram



Often, especially in scenarios similar to the above process flow, lack of transparency of risk management results or inputs can be one of the main challenges for teams. Information security teams may not be passing along all the necessary information needed for risk remediation – or the reciprocal may also be true.

Opportunity: Communication is Key

- **Be sure to use your risk prioritization framework! –** After deciding upon a risk scoring framework, simple or complex, it is critical to drive awareness and usage of this prioritization system. Teams may receive a blanket list of risks or vulnerabilities and not have the context of the framework that a separate information security team has decided upon.

- **Practice "DevSecOps"** – The same issues of separation of team and process that historically plagued development and operations teams (leading to the concept of DevSecOps teams) can also be found in security processes. DevSecOps aims to bring security practices (i.e. risk remediation) into normal BAU for your product and service teams leading to a more streamlined form of the process flow above.

- **Embrace Automation** – Automation of risk remediation workflows can be seen as a costly upfront process – but can often be a positive ROI for mature cybersecurity organizations. Risk remediation throughput time can often be held back simply by dead periods between remediation workflows (often with applicability to other IT-centric parts of the business). In addition to tools, you need to develop a culture of automation with resources who are dedicated to this function i.e., identifying high volume low complexity "transactions" that can be automated, estimating benefits, implementing and then maintaining.

Reliable and Useful Metrics

Challenge: Telling a "Good" Risk Remediation Story

As your teams begin to streamline the risk remediation process, one challenge for many InfoSec orgs is to demonstrate to leadership that their actions have successfully reduced the risk profile of their organization. Unfortunately, many teams may not know where to turn in terms of useful metrics that tell a compelling story. It can be very easy for security reporting to actually paint a bad picture, rather than one of transformative and continuous improvement. Any reporting, security or otherwise, will aim to promote transparency and clarity, as even bad results can be an opportunity to understand where roadblocks or conflicting priorities may be impeding progress.

Opportunity: Understand Your Audience

- **Identify Key Metrics -** The first form of risk remediation reporting for most organizations is a status of burndown to all risks; however, this may not paint an accurate story. Focusing on specific metrics such as average time to remediate like-vulnerabilities or zero-day specific burndown can be more useful to determining areas for process improvement or an actual reduction to information security risk.

- **Separate Reporting by Role –** The reporting metrics that are useful for executive leadership (e.g. risks by business area) may not be as useful to your teams on the ground. Focusing on metrics that allow for drill-down capability (e.g. count of vulnerability X for a specific team) can help that team to focus on their own specific roadblocks and how those can be turned around for a more successful process

- **Mix in Proactive Reporting –** Lagging indicators like remediated risks can be good for showing progress, but a next evolution of reporting may include metrics on actions performed for risk root causes. Highlighting progress made on fixing the root cause of common risks or vulnerabilities can paint a great picture for leadership that your information security team is being forward thinking in their security activities

Immediate Steps to Improve Your Risk Remediation Capabilities

Information Security teams across all industries likely face many of these similar challenges and the first question often is "What Can I Do Today?" The best answer is that developing a sustainable and successful risk remediation program is a long-term initiative and requires buy-in from teams across the full risk management lifecycle. However, there are key steps that can be taken by information security teams in the short term that can show measurable results in terms of an organization reducing its risk profile

1. Ensure any manual risk identification methods are baselined against company security policy

- Ensure company security policies and standards are both up-to-date and practical
- Organizations need to be sure they are testing against these policies; not against the entire world of cybersecurity
- Policies should be designed with your organization's risk tolerance in mind

2. Ensure risk assessment methods and prioritization methods are published and understood

- Organizations may miss risk findings due to lack of awareness by the proper remediation teams.
- Understand all methods of risk identification first to more efficiently burndown a risk backlog

3. Ensure your security team is using an industry standard risk scoring system

- Quantifying a risk as simply “High, Medium, Low” can be deceiving
- Industry standard scores like the Common Vulnerability Scoring System (CVSS v2) provide a granular 0-10 scale
- CVSS 2 can also provide the granularity needed within “High” level vulnerabilities

4. Simplify reports to include only role-based metrics

- Senior leadership often requires “binary” forms of reporting or want to view simplified trend lines over time
- However, a more useful form of reporting for InfoSec or delivery teams may show detailed information tailored specifically to their risk profile and attack vectors
- Automating these reports, where possible, helps to ensure reconciled data for information security teams operating in the middle

Leveraging these key tips, as well as ensuring your information security teams have the proper resources and business alignment, can help to streamline risk remediation and decrease the cybersecurity risks posed by a variety of bad actors.

(1) 53% of IT professionals said security will be a top budget priority in 2018. “2018 IT Budgets: Spending priorities, funding changes, and status with the organization” Tech Pro Research. September 2017

(2) It may take 2-17 minutes to remediate each individual instance of common application vulnerabilities. “Remediation Statistics: What does Fixing Application Vulnerabilities Cost?”, Denim Group, Ltd. – Presented at RSA Conference 2012

About the Authors

Justin Whitaker is a Partner and Practice Lead of DayBlink Consulting's Cybersecurity Center of Excellence and is based in the McLean Virginia office.

Jacob Armijo is a Senior Consultant within DayBlink's Cybersecurity Center of Excellence and is based in the McLean Virginia office.

Please direct questions and comments about this report to cyber@dayblink.com

About DayBlink

In today's cybersecurity environment, the threat landscape is rapidly evolving. It's outpacing the current defensive resources and skill sets of most corporations – meaning many companies are falling victim to attacks by malicious agents.

The way we do business is also changing – with more data stored, living in the cloud, and constantly demand on the go. Breaches can mean losing clients and customers overnight.

DayBlink works with clients to improve their security posture. We assess threats and vulnerabilities, identify organizational risk, prioritize remediation efforts, and implement solutions to secure IT environments and critical assets from sophisticated cyber-attacks.

DAYBLINK

For more information:
Visit: **www.dayblink.com/services/technology/cybersecurity**
Email: info@dayblink.com
Call: 1 (866) 281-4403