WHITEPAPER

How Organizations With an Emerging Cybersecurity Program Can Accelerate Risk Reduction

LevelBlue

When cybersecurity programs are mature and firing on all cylinders, the security functions of an organization go beyond preventing attacks and breaches. They become business enablers, aligning and allying with the other divisions of the company to achieve strategic, operational, and revenue goals. The most effective and mature cybersecurity organizations are completely aligned with business priorities to help manage and reduce risk based on what matters most to the business.

Less mature cybersecurity organizations that haven't yet grown into that enabler role need to chart a path to get there. What should that path look like? Cybersecurity teams should be accelerating risk reduction in a way that lines up with business goals and constraints on budget and resources. This often requires systematic changes in processes, controls, and culture across the security organization.

While these less-mature cybersecurity organizations can certainly accomplish a lot of that through internal efforts, sometimes they need a boost from trusted third parties to help them fully achieve their goals.

Cybersecurity consultants can help identify and establish essential elements of emerging cybersecurity programs, from strategy, governance, and enterprise risk management to controls architecture, implementation, and management.

Working with consultants and other third-party experts can help security leaders plan for the investments that will make the biggest impact on their cyber risk posture. With the right methodology and expertise, independent consultants can also help organizations overcome technical challenges, execute on new strategies, and accelerate cybersecurity maturity gains.

Understanding Cybersecurity Maturity

Cybersecurity maturity models typically provide a scale or curve upon which an organization can be scored based on a defined framework of characteristics or capabilities. The National Institute of Standards and Technology (NIST) offers one of the most popular of these, the NIST Cybersecurity Framework (CSF). CSF provides a security framework upon which security maturity can be measured. The framework is built around five areas: identify, protect, detect, respond, and recover.

In a benchmark study, The Relationship Between Security Maturity and Business Enablement, analysts with Enterprise Strategy Group (ESG) found that leading organizations—those with the highest maturity levels—tended to be the furthest along in all five functions of the NIST CSF.

Meanwhile, following organizations—those with less maturity—struggled with one or more areas of NIST CSF, particularly in categories like threat detection and incident response. The study showed that these organizations were missing key risk management processes and practices. When they did have those practices in place, they were frequently ad hoc. This means they weren't regularly reviewed, weren't repeatable, and weren't adaptable to business needs.

Based on a survey of 500 organizations, the study statistically showed that the security maturity levels can have marked implications on both security readiness and business performance. Consider the following:

- Leading (greater maturity) security organizations were more than 2x as likely to report improvements in their cyber risk posture over the last 24 months as following (less mature) organizations.
- Leading security organizations were more than 2x as likely to be seen as an enabler to line-of-business stakeholders as following organizations
- Following security organizations were more than 5x as likely to be seen as a roadblock to line-of-business stakeholders as leading organizations.

This suggests that if following organizations can work to boost their security maturity, they'll (1) not only build more effective systems for accelerating risk reduction, but (2) will also be better able to instill in the minds of executives and line-of-business leaders that the security function is a driver of business innovation and growth.

Leading (greater maturity) security organizations were more than 2x as likely to report improvements in their cyber risk posture over the last 24 months as following (less mature) organizations.

Steps for Maturing Your Security Program

The study also found another hallmark difference between leading and following organizations. Leading organizations are better able to understand the business impact of threats and vulnerabilities to critical business assets on the network—and use this knowledge to prioritize how they respond to these risks.

All of this suggests that in order to accelerate a move up the maturity scale, less mature security programs would be well served to:

- Gain basic visibility into the organization's cyber-attack surface and what that means for business risk
- Observe business priorities and existing security controls to assess current risk levels
- Establish and regularly review formalized and documented policies and processes to prioritize highest risks to the business
- Establish security awareness throughout the business

- Create opportunities for conversations with executives and line-of-business stakeholders about what security risk means to the business. Security programs that are further down the maturity curve can make progress on these points of improvement through several key initiatives—all of which can be expedited through the expertise of an experienced security consulting team.

Information Security Risk Assessments

Information security risk assessments evaluate the business missions that a security program must support, the risk environment in which the business operates, the controls currently in place, and the cyber risks most likely to materially impact the business.

A comprehensive cyber risk assessment not only identifies mission-critical services and data, it can help prioritize the biggest risk gaps in securing those services and data.

Many organizations engage a third-party advisor for help with a cyber risk assessment. They want candid and expert analysis of the organizational posture, as well as an external voice that is removed from company politics and that can offer trusted guidance to IT and line-of-business decision-makers. These trusted advisors and security SME's also bring to the table deep expertise in assessment frameworks like NIST CSF, as well as regulations for relevant industries or regions.

Conducting a cyber risk assessment through a consultant also helps start a meaningful security conversation within the organization by:

- Providing an unbiased, third-party comparison of an organization's baseline to its industry peers
- Offering insight into inherent risk across the business and determining residual risk
- Identifying the priority of security controls that need to be implemented in order to help mitigate the most significant risks to the business first, based upon risk tolerance
- Using a framework like NIST CSF to measure progress in risk reduction after the assessment as compared to industry peers

Risk Management and Zero Trust: How to Get Started

In addition to broad risk assessments, consultants can also help a less mature organization understand its readiness for important security initiatives, such as a drive to become a cloud-first company or the deployment of the zero trust security principles in their environment. Less mature organizations may want to work their way toward the flexibility and business enablement of zero trust security, but they will first need to understand their current security posture, architecture, policies, and culture in order to successfully evolve.

Because there are so many components to executing on zero trust security principles, less mature organizations may not yet have the expertise and experience to fully do so. Through a zero trust readiness assessment, consultants can help organizations understand the next steps they'll need to take, technically and organizationally, to move toward that zero trust model, including the resource and skills gaps they'll need to fill.

Relevant Services from LevelBlue:

- LevelBlue Risk-Based Cyber Posture Assessment

The initial information gathering in a risk assessment should then be matched against your organization's framework of choice and the regulatory requirements of the business. This highlights residual risk and identifies the gaps between existing security controls and what is needed to appropriately manage risk and close the gaps. This should all be compiled into a final report. This report can help guide the organization's investments and next moves.

When considering a third-party for your risk assessment, make sure the consultants doing the assessment gather information and documentation in 3 key areas.

Business Functions and Requirements

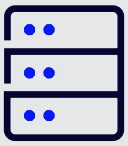
Regulatory and business requirements that your information technology and infosecurity team supports, primarily discovered through:

- Interviews among key business and technical stakeholders

Architecture

The existing IT and security technology and architecture that makes up the organization's current IT environment, primarily discovered through:

- Interviews
- Conducting tech inventories
- Collecting documentation of data flows and standards



Controls

Security controls, policies, and processes, primarily discovered through:

- Documentation and evidence collection
- Technical testing
- Interviews
- Conducting a tools and technologies review

Cybersecurity Awareness and Training

A high degree of cybersecurity awareness across an organization plays an important role in cyber risk management. It helps minimize the risk of employees unwittingly becoming victim of phishing attempts and other social engineering tactics that expose the organization to malware attacks and breaches. This is particularly important in the face of remote workforces targeted by adversaries seeking to prey upon trends. Educating employees makes them aware of phishing and attack trends. It helps prevent them from becoming an unwitting entry point for an attack. When done well, it also turns employees into the first line of defense when it comes to spotting phishing attacks and other potential threats that present themselves at the endpoint level.

This is why investing in security awareness through systematic employee training can stand as one of the highest ROI methods for allowing security programs to help reduce cyber risk across an organization.

Before developing training materials and programmatic training, organizations need to understand the baseline at which employees are operating. Security consultants can help establish this through testing cybersecurity knowledge across your organization. Additionally, organizations may want to consider doing social engineering tests, such as conducting phishing simulation testing, to see how well employees are recognizing malicious messages.

From there, a consultant can help develop custom security training content that targets the business needs. Ideally an organization should find a way to pair multimedia content with ongoing awareness testing as the employees progress through lessons on a regular basis.

Ideally, an organization shouldn't be reinventing the wheel when creating security training materials.

Security engineers aren't instructional designers and shouldn't be expected to have that skill set. Consultants and service providers can offer customizable modules that make it possible to tailor training content without an onerous amount of work.

As training progresses, a good security-awareness program should also be able to track the effectiveness of the training. It should also test employee behavior enterprise-wide, as well as provide a reading of how effectively security is embedded in the culture of the organization. And that goes for all lines of business, including C-suite executives, and within the finance group.

In terms of maturity and IT cybersecurity teams being aligned to business objectives and outcomes, cybersecurity consultants can help. They will guide organizations as they navigate business stakeholder objectives and rally support for this kind of across-the-board training and testing of employee security awareness, including building the business case for the program. All of the information about your employee behavior during assessment can help feed training curriculum and regular communication between the security program and employees at large.

Relevant Services from LevelBlue:

- Social Engineering Training
- Vulnerability Assessment
- Phishing Simulation Platform
- Security Awareness Training

Common Themes in Cybersecurity Awareness and Training

- Acceptable use of systems
- Data handling
- Social engineering awareness
- Phishing awareness
- Physical security
- Social media dangers
- IoT use policies
- Software installation policies
- Protocols around handling
- Regulated data
- Password security
- Cloud use policies

Threat and Vulnerability Management

Understanding and managing system configurations and vulnerabilities across the network is a key part of identifying and managing cyber risk—and aligning security priorities so they help to enable business.

To do this effectively, an organization needs first to gain visibility into its network assets across multiple environments. Visibility is key. It helps establish a program for threat and vulnerability management that prioritizes mitigating vulnerabilities and misconfigurations based on business risk. It's achieved by:

- Identifying and mapping assets and the importance of data on them, as well how they serve the business
- Mapping the technical details of those assets, including operating systems, ports, and services running on every device
- Tracking vulnerabilities and misconfigurations on those systems
- Prioritizing for mitigation of the vulnerabilities that pose the highest risk (which may not always be the common vulnerabilities and exposures [CVE])
- Patching vulnerabilities or mitigating through other means, such as changing security policy to block an exposed vulnerability based on priority

Every connected IT device that an organization uses, and every software platform it depends upon, exposes the infrastructure and the business to at least some level of risk. These risks could come from any number of vulnerabilities: software flaws, configuration errors, overly permissive access, business logic flaws, and more. The key to sound threat and vulnerability management is minimizing the exposure level wherever possible. To do this, an organization needs to mitigate the highest risk (most exposed and exploited) vulnerabilities that exist within these technologies. The greater the danger posed by a vulnerability, or the importance of the asset at risk, the higher the priority to mitigate.

Relevant Services from LevelBlue:

- Vulnerability and Threat Management

Cybersecurity consultants are skilled in helping organizations set up threat and vulnerability management programs that:

- Identify vulnerabilities and threats through comprehensive vulnerability scanning and analysis
- Enhance visibility into business risk by aggregating context about assets and vulnerability to establish data-driven prioritization
- Accelerate meaningful remediation by deploying controls with low false positives, and by relying on threat intelligence that makes recommendations based on current threat activity

Prioritization is key, because software flaws alone are discovered by the tens of thousands each year. Coalition's Cyber Threat Index 2024 forecasted a 25 percent rise in common vulnerabilities and exposures in 2024, equating to nearly 34,900 vulnerabilities. This risk surface has been exacerbated by remote workers with new endpoint devices, and increased reliance on emerging technology such as IoT, 5G, and edge computing.

Because it isn't possible to fix every vulnerability in an environment, organizations need to make choices through a risk management exercise that ties technical visibility back to the priorities set during risk assessment—focusing on the most critical applications to the business.

Penetration Testing

Getting a broad view of existing vulnerabilities is a crucial first step to managing risk. It doesn't end there. Organizations also need to understand how attackers use these flaws to attack an environment.

Penetration testing (pen testing) is a way to see how outside attackers can operate within your existing infrastructure. Sometimes referred to as offensive security, the idea behind penetration testing is to task internal or third-party white hat hackers to break into systems the way attackers would in the real world.

Penetration tests probe beyond the scope of automated vulnerability scans. They can find gaps in protection that can arise when unique combinations of applications, systems, and security defenses work together in live environments, including:

- Business logic flaws
- Weaknesses in processes
- Gaps in employee training

Additionally, these tests help satisfy certification standards requirements for Payment Card Industry Data Security Standards (PCI DSS).

Relevant Services from LevelBlue:

- Penetration Testing Services
- Adversary Simulation Services

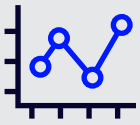
Pen testing consultants work within limited rules of engagement. These are defined by the scoping at the beginning of the engagement. An engagement generally works in three stages:

Scoping

This determines the test methods, frameworks/tools used by testers, as well as where in the network or physical premises they will work.

System Probe/ Compromise

Penetration testers try to gain access and maintain access while evading detection to see how their client's security measures are really working.



Analysis

Most importantly, pen testers provide written analysis on the vulnerabilities they exploited, and what that means for an organization trying to improve its defenses.

Experienced pen test consultants understand that this final step of analysis and recommendation is how pen tests provide true value to a program. Consultants can help organizations understand how to use the results to drive their future roadmap that directly counters the attack tactics techniques and procedures (TTPs) used by the white hat hackers during the pen test.

Working with a Cybersecurity Consultant: Taking the First Steps

Consulting engagements can help with the following for cybersecurity organizations

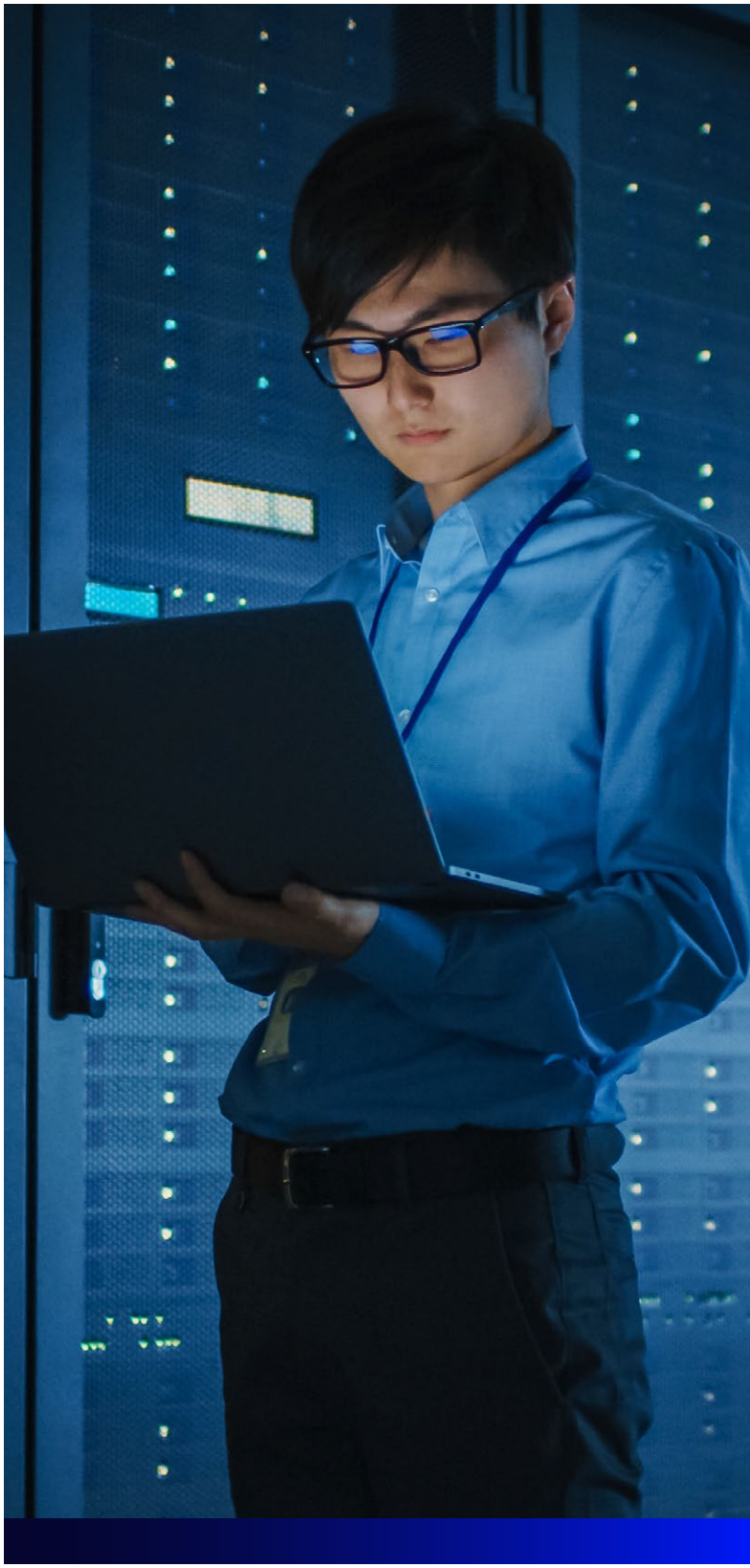
1. **Establish a baseline for where the organization's biggest risks are,**
2. **Create a strategic road map for how to phase the deployment of key security processes, policies, and controls, and**
3. **Make recommendations for rapid improvements.**

Starting first at risk assessments, and using the foundational elements described above, establishes ground-level controls—a solid base from which more advanced initiatives can be launched.

A reputable security consultant can be an invaluable ally for security organizations as they build and refine a cybersecurity program that helps with elevating their cybersecurity posture and maturity to better align with business objectives and outcomes. Engaging with a consultant:

- Helps accelerate improvements by helping to break down silos within the IT group and other lines of business
- Brings industry and regulatory expertise and relevant experience to the organization without a strain on payroll or recruiting
- Provides an unbiased view of your current program and operational risks
- Adds credibility to arguments for organizational change and/or additional investments

Most importantly, consultants can help start honest conversations between security and business executives about the relationship between cybersecurity investments and business performance.



LevelBlue

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.