WHITE PAPER

5 Critical Steps to a More Mature Security Posture

The world is changing. For organizations, digital transformation is setting a rapid pace, bringing with it new opportunities but new threats and risks too. In reaction to both the opportunities and the risks, governments around the world are increasing regulatory compliance requirements and tightening up legislation related to data privacy (like the introduction of the General Data Protection Regulation (GDPR) in the EU).

Secureworks®

Introduction

For many companies, their security posture is being left behind, stuck in a defensive and preventive posture that leaves them unable to detect and respond appropriately. For too long, security has been reactive, focused on product releases that lead to overly complex product stacks that serve to complicate, rather than reduce, risk.

Aligning the maturity of an organization's security posture with the risks it faces is no longer optional, or just an aspiration for the biggest budgets. Security is a business risk issue, and reactivity is no longer enough. Emerging, high profile issues like ransomware often trigger a reactive posture where the emphasis is on reviewing a checklist of specific 'known' threats and risks. In fact, being resilient to a breach is dependent on an integrated set of solutions and controls, instrumented for visibility across the whole environment, and made effective by people who follow the right policy, process and procedures to manage them. Technology based defense in depth must now be replaced by defense in concert, where all elements of cybersecurity work together, based on risk-prioritized goals.

This paper sets out to explain how to move through five key stages that you can tailor to your organizational needs – Plan, Buy In, Execute, Evolve and Future Proof. It contains vital information and proactive strategies that may be valuable to organizations at all stages of cybersecurity maturity and will assist you in assessing what you can do alone and where you need help. This paper discusses both tactical improvements for less mature growth companies and strategic integration of cyber risk management for larger enterprises.

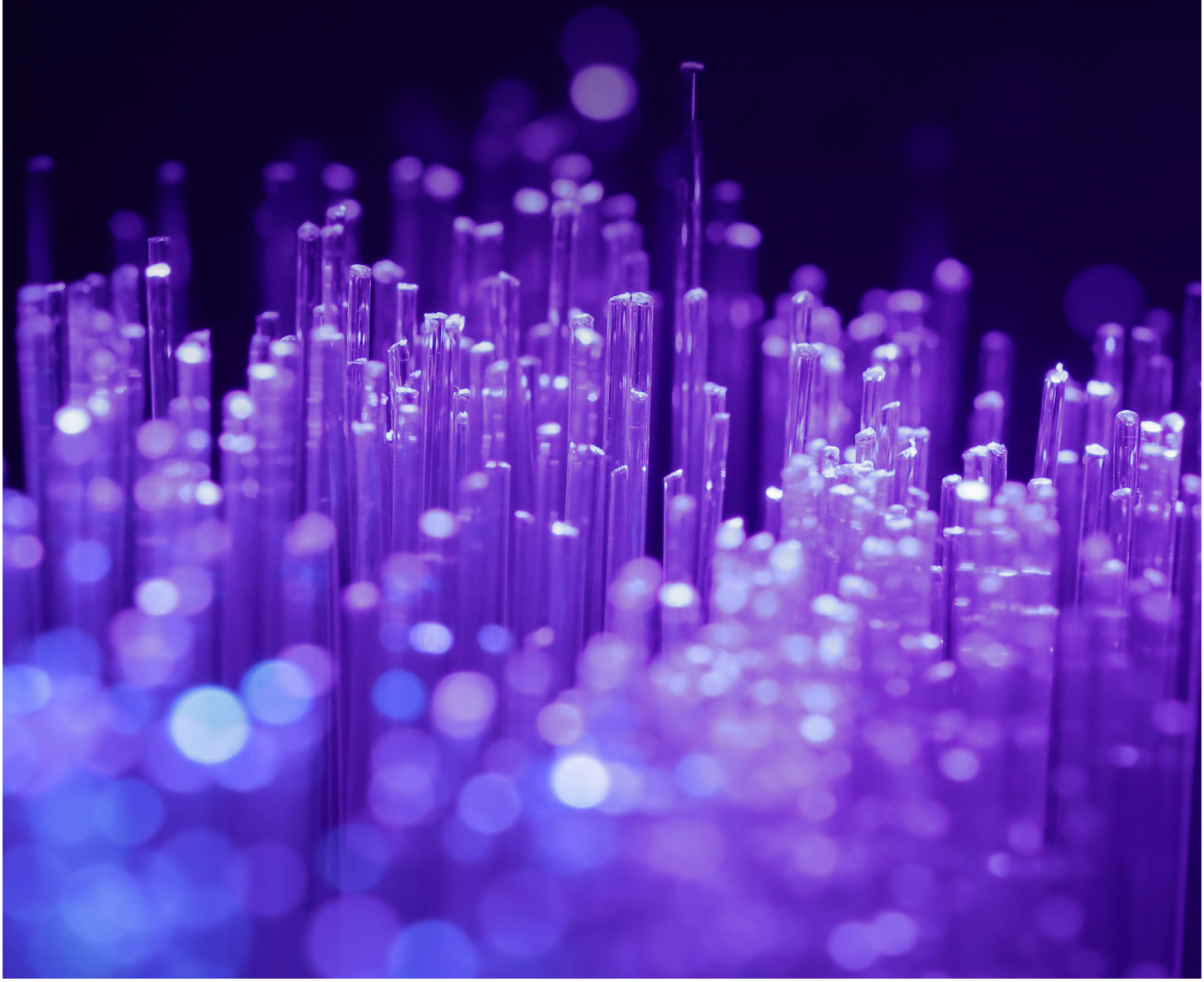
What You Will Learn

- Why cybersecurity must be treated as a key element of business risk
- How defense in concert improves on defense in depth
- What to say to your C-Suite and executive committee to gain buy-in and budget

Who Should Read This White Paper

- CEOs/ C-level executives
- CISOs/CSOs
- CIOs
- Directors of Security/IT

To create an effective cybersecurity program, you must first develop a strategic and overarching view of your organization's priorities, critical processes, and assets followed by identification of the organization's security needs.



ONE

Plan - Based on Risk

To create an effective cybersecurity program, you must first develop a strategic and overarching view of your organization's priorities, critical processes, and assets followed by identification of the organization's security needs. This is your cyber-business risk model. This paper will start by providing seven key steps to developing a cyber-business risk model relevant to your organization.

Steps to Developing Your Cyber-business Risk Model

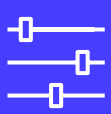
1. Agree on business needs, objectives and tolerance

2. Get to know your data

3. Understand the threats

4. Select a framework

5. Document current state controls



6. Identify top business risks

7. Develop a timeline to address security gaps

Secureworks

1. Agree on Business Needs, Objectives and Tolerances

There are multiple reasons why your organization might embark on establishing a more mature security posture. Whatever the reason, it is impossible to make informed decisions about security strategy and tactics without first understanding what you are trying to achieve as a business, why you want to achieve those goals and what constraints you will face.

It is impossible to make informed decisions about security strategy and tactics without first understanding what you are trying to achieve as a business.

These issues may vary by size of organization, industrial sector, organizational structure, technology in use, regulatory environment and many other factors.

To take an example, Company X, thanks to rapid growth and regulatory change, needs to better protect the personally identifiable information (PII) it holds. Its new Chief Counsel has asked the CIO to review cybersecurity and provide a plan to improve the company's cybersecurity posture.

The CIO determines that the business need is to 'introduce controls to reduce the risk of lost or stolen PII which subsequently reduces the chance of a data breach occurring and hence breaching government regulation.' This is more than just saying 'stop the organization being hacked' as it provides the need, the requirement and the consequences of not acting.

2. Get to Know Your Data

Once you have established your business need, you can start to build an understanding of the data you need to protect - who owns it, where it is stored and how it is processed. The data life cycle involves multiple stages - creation, application, transmission, storage, archiving and destruction.

Creation — Maybe your organization is generating a database of personally identifiable information? Perhaps it is intellectual property generated by research and development teams? Whatever the creation process, knowing what kind of data is being created is important. So is knowing who is creating it and who is using it, in order to understand their impact on organization cybersecurity.

Application — How does the data you collect or create impact your applications? What systems are being used to collect the data, what systems are processing the data and what systems are protecting the data?

Transmission — How is the data being sent between applications and data users? Is it being sent in email? Is it hosted on a shared drive that everyone has access to? Is your organization applying tokenization to the access of the data? Is encryption applied to the data during transmission?

Storage — Where is the data being stored in your network? Is it in one location? Perhaps it is outside of the organizations boundaries, such as in cloud services. Perhaps your organization has multiple departments accessing the data and storing it in different

locations. If this is the case, does your organization know who has access to the data and how they might be storing it? It is often the case that multiple users are saving the same data in multiple places in a single network.

Archiving — Once the data is no longer being used, how is it archived? Is it on tape backup drives, and would this type of drive be easily accessed if needed? Is the data archived in a single location or multiple locations in your network?

Destruction — Once you determine the data that is no longer being used, do you have a process in place to destroy the data? And, of increasing importance, can you verify that it has been destroyed?

Understanding the data lifecycle vastly helps organizations to grasp the relationship between data lifecycle and the organizations critical business processes. Understanding this relationship can highlight the areas of risk between the two and allows organizations to fortify necessary defenses for that which is critical to their operation.

There is a lot of complexity in the data life cycle and no two organizations are alike. In our example, Company X is using a web application to collect other organizations' employee information. It is creating a database of PII details that are associated with user names and passwords, this database will be a critical business process for Company X's success. The systems in scope here are the web application and the database it uses. Its marketing department is using some of these details to determine client profiles, by extracting data from the database in spreadsheets, storing it on their machine and uploading it to a cloud-based marketing system. Has the marketing department established a shadow IT function that is storing the data in a separate location? How is that data being archived and destroyed when it is no longer needed?

3. Understand the Threats

No two business are alike in the types of threats they face, so it is vital to define the attack vectors and threat profile for your specific organization. Doing so will allow meaningful security conversations between security teams and senior management, as control improvements and vulnerabilities can be tied to actual risk to the business. Potential threat actor categories include nation states, insiders, hacktivists and terrorists. However, the biggest threat group for most organizations is cyber criminals, organized crime groups who leverage cyber threats for monetary gain. Attacks may target specific organizations or may be widespread commodity attacks, including ransomware and trojans. Targeted attacks may directly steal money, or assets that can be sold (e.g. personal data, credit card data, intellectual property). They may gain entry via third parties with access to the organization's system, as in the 2013 Target attack where millions of credit card details were stolen for sale on the black market.

The core threats organizations face are often unchanged year on year, but the tactics used by threat groups to achieve their aims can often change. Ransomware, such as WannaCry, has been a key trend over the last three years for crime groups trying to

make money. Threat actors are entrepreneurial in the way that they respond to market forces and chase ROI. The growth in value of cryptocurrencies such as Bitcoin has recently lead to a spate of cryptocurrency mining attacks. Next year may bring new tactics.

Knowing which threat scenarios pose the highest risk to your organization requires self-assessment. Partnering with an independent threat intelligence company will ensure your focus is on protecting against current and relevant threats.

4. Select a Framework

Organizations that want to ensure that they put the correct controls in place baseline against an established security framework such as NIST Cyber Security Framework, CIS Critical Security Controls or ISO 27001. Some industries, such as retail, will require adherence to sector specific frameworks such as PCI-DSS. Doing this can also assist considerably towards complying with newer regulatory regimes like GDPR.

Organizations are also leveraging proprietary security frameworks and maturity models that encompass the different regulatory and industry good practice requirements. It is important though to understand that framework compliance should be viewed as a minimum rather than the ultimate goal.

It is important though to understand that framework compliance should be viewed as a minimum rather than the ultimate goal.

5. Document Current State Controls

Once you understand your organization's data and data life cycle, and the threats you face and the framework you are aligning against, you can then start to determine your weaknesses and gain an understanding of where you are most vulnerable. You will need to understand what controls you already have in place and the ensuing vulnerabilities before you can work out how to improve those controls.

To do this, examine four factors in your organization; the people, process, policy and technology. The findings in each of these areas should form the basis of documentation of current controls you have in place and the vulnerabilities that result.

People: Are your end users aware of your organization's cyber strategy and mission? Are they using strong passwords and regularly changing them? Do people involved in handling data understand your data handling policies?

Process: Do you have effective processes to monitor for and detect threat activity? Do you manage user access permissions appropriately? Do you identify and remediate vulnerabilities in your systems? Processes are the benchmark of a mature security posture; these are just some examples.

Policy: What are your organization's policies based on your network and data life cycle? Have you established policies related to the management of third parties and their access to your data?

Technology: Do you have the appropriate technology in place to enable effective security processes, while preventing malicious activity? Many cyber-attacks are only possible because systems, networks or applications contain vulnerabilities that allow unauthorized people to gain access to them. The security leader should ensure that the infrastructure is designed and built with security in mind. However, new vulnerabilities are being discovered all the time. Regularly scanning and testing your environment for vulnerabilities, and applying timely updates, is just as crucial to reducing the risk of a successful attack.

6. Identify Top Business Risks

Now you can align the threat vectors you face to your known weaknesses and develop an organizational threat model.

Revisiting our working example from earlier, Company X has concerns that their staff could be mishandling data, saving it to USB keys and separate hard drives. The data they hold could be of interest to opportunistic criminals. They have also discovered that there are weaknesses in their web application that could be exploited. So, Company X might map potential threat vectors and their motivations against their weakness and produce the table shown in Figure 1, which highlights that the two top threat vectors are insider threats and opportunistic criminals. It also highlights that the threat would likely come via weaknesses in their people and their technology.

Threat Vector (and Motivations)/Weakness	People	Process	Policy	Technology
Nation States Steal intellectual property to provide competitive advantage to their companies	Low	Low	Low	Low
Insiders Employee and 3rd-parties who cause data breaches through intentional or unintentional actions	High	Low	High	Medium
Hacktivists Tarnish brand to make political points based on group motivation	Low	Low	Low	Low
Terrorists To cause destruction, damage, or harm through cyber activities	Low	Low	Low	Low
Opportunistic Criminal Groups Leverage cyber threats for monetary gain	Medium	Medium	Low	High

Figure 1

Understanding these threats, vulnerabilities and your assets allows you to calculate the risks facing your organization.

Cyber risk may form one aspect of business risk but there is no doubt that it is becoming an increasingly important one, as Boards and C-level executives become more aware of the potentially catastrophic results of a security breach. The outcome may include regulatory fines, collapse in share price, reputational damage, loss of customers and more.

This, combined with regulatory changes and growth in emergent technologies, means that approaches to cyber risk are starting to become more sophisticated and more critical to the success of a business. For example, there is a move towards assessing 'cyber value at risk', an approach originating in measurements of financial risk that considers amount of loss, probability of loss and timeframe. Organizations with greater cyber security maturity and awareness are seeking continuous risk assessments rather than occasional snapshots.

The compliance landscape, driven by the EU General Data Protection Regulation (GDPR) is becoming more risk focused rather than based around one size fits all compliance checklists. And new technologies like IoT and connected cars are driving a need for highly specialized risk assessments tailored for threats that could have life shattering impacts.

7. Develop a Timeline to Address Security Gaps

From this point, your organization can start to develop a prioritized timeline for achieving their goals. Using a timeline to success means an organization addresses high priority issues first by focusing on the most critical vulnerabilities and threat vectors, working down to the lowest priority.

Showing that you understand your data and data lifecycle, demonstrating the weaknesses in your current cybersecurity posture and detailing a phased approach to dealing with those issues will drastically increase your chances of gaining executive sponsorship and support and an appropriate budget.

In our worked example, Company X develops a 3, 6 and 12-Month plan which addresses the highest risks in the first 3 months, medium risks in 6 months and the remaining requirements after 12 months. (See Figure 2.)

Figure 2: Phased roll out of security strategy

It is the responsibility of the CISO or executive in charge of cybersecurity to ensure that Board or C-level executives understand the cyber risks to the business, how well those risks are being managed and what is required to ensure that they are managed properly.

TWO

Achieve Buy-In and Budget

The previous section mentioned that you may need to obtain Board or C-Suite level buy-in for the implementation of a phased remediation plan.

It is the responsibility of the CISO or executive in charge of cybersecurity to ensure that Board or C-level executives understand the cyber risks to the business, how well those risks are being managed and what is required to ensure that they are managed properly.

Research conducted by the Ponemon Institute[1] shows that only 33% of Board members claim to be knowledgeable about cybersecurity. It is vital, therefore, to build a good relationship with the Board, to devise and implement a successful reporting process and to present this information in a way that:

- Is accessible for non-technicians
- Uses business language rather than technical jargon, avoiding acronyms
- Is specific to the organization in question and the threats it faces
- Aligns with business priorities
- Makes the case for cybersecurity as a key enabler of business goals and strategy rather than an optional cost.

33%
of Board members claim to be knowledgeable about cybersecurity according to research conducted by the Ponemon Institute.

To lay the ground for this information to come across successfully, it is important to prepare. That means doing your research on existing Board experience, preconceptions and perspectives. Time spent creating one-to-one relationships with Board members in advance of the presentation is time well spent. In particular, attempt to engage in advance with the chair of the Board committee with primary responsibility for cybersecurity risk, whether that be the Audit or Risk committee, or a special committee dedicated to IT, information security, or data protection.

CISOs should also take every opportunity to educate, using the language that the C-Suite will understand – the language of business. Cybersecurity breaches in the news can also be used as an impetus to explain how a breach happened, including the result of forensic investigations, threat actor motivations, and a layman's overview of the techniques, tools, and procedures used. Effective storytelling will enable you to successfully demonstrate how the breached company became vulnerable to the threat and what your organization does differently—or could do differently—to avoid becoming a victim.

[1] Defining the gap – the cybersecurity governance study, Ponemon Institute, June 2015 http://www.companydirectors.com.au/~/media/resources/director-resource-centre/glc/board_of_directors_cybersecurity_governance.ashxa

Figure 3: **Dos and don'ts of board reporting**

What Not to Report	Consider Instead
Acronyms	Full names and descriptions
Technical and security jargon	Business terms and a common language for every meeting
Tactical plans that tell how security works	Strategic plans that demonstrate why security is a means to a business outcome
A problem with no solution	A realistic roadmap for improvement
Metrics without measurement	Replicable metrics that track trends
Data without business relevance	Financial, operational, reputational, and regulatory concerns that align with Board oversight responsibilities
Too much data	Only data that has strong business relevance

It is key to ensure that any presentation aligns with and leads with Board concerns i.e. business impact. One of the main benefits of the Planning stage is that it enables you to tie security investment to actual business risk; every investment can be shown to mitigate a particular threat that's relevant to the business context. To exercise their fiduciary duties, they need to know, with confidence, that the risk is being managed. That means they care deeply about the impact a breach could have on innovation, productivity, revenue, reputation, and shareholder value.

So, avoid getting bogged down in technical detail and tactical issues. Instead focus on business outcomes that impact current or future revenues and margins and the effect on organizational resilience.

Consider asking questions that lead to a discussion on how to prioritize resources in a way that has the greatest impact on risk mitigation. It may help to present several investment options that articulate the trade-offs that have to be considered when it comes to allocating resources. Time spent on preparatory research in one-to-one discussions, as mentioned above, may help in pitching these at a level that will be acceptable.

It is also important to remember that with 'people' forming one of the four areas of potential vulnerability, it is not just senior business personnel who need to buy into security. Forming a steering committee with representatives from different parts of the organization so that they get regular updates on what's being done around cybersecurity and why. It is a great way of enhancing buy-in. So is putting together a communication program to all employees so they understand their role in protecting data. Creating a security aware culture will be discussed in greater detail later in the paper.

Today's threats, commodity or otherwise, target between the layers to exploit small gaps—in technology, processes, and security hygiene—leaving you vulnerable to breaches. Even if you're well protected from one type of threat, you're probably vulnerable to others.

THREE

Execute – for Maturity and Defense in Concert

By this point you should now have a prioritized plan to enhance your security maturity based on your cyber-business risk model. You've gained Board or C-Suite backing. You are ready to execute.

But before you start, you need to be sure you are executing for security maturity.

There are two elements to highlight here.

- First, you need to remember that a mature security posture goes far beyond tick box compliance. Being compliant is necessary but it is not the same thing as being secure. The goal is an organization-wide culture of security from the top down that helps to reduce overall business risk and improve the company's security posture, while also meeting regulatory requirements.
- Second, if executing your prioritized plan involves buying large amounts of new equipment and focuses on defense in depth, it is time to stop and assess whether that will really provide the security maturity you require. Today, rather than defense in depth, security maturity requires defense in concert.

Traditionally, executing a security plan would have involved ticking the compliance check boxes by building up layers of defenses across your networks, endpoints, and applications, and in the cloud, hoping that these multiple layers would keep you safe.

That might have meant strengthening individual areas of defense, going in depth on things like detection with layer upon layer of technology.

One problem with this is that you have to continually replace what you have when something new comes on the market. That's not fiscally sound or even always feasible. It is fragmented and unwieldy. It may be particularly ineffective without adequate skilled resources to work with the tools, a challenge given the difficulties of recruiting cybersecurity experts. And it may also be hindering your ability to innovate and grow.

And worse still, it doesn't always protect you.

Today's threats, commodity or otherwise, target between the layers to exploit small gaps—in technology, processes, and security hygiene—leaving you vulnerable to breaches. Even if you're well protected from one type of threat, you're probably vulnerable to others.

All those point products must be managed, updated, and monitored. We weren't surprised to see that one enterprise client had seventy plus of them. This is not only expensive, but these products are all generating thousands—or millions—of alerts every day. It is virtually impossible for overstretched and understaffed SOCs to review all the alerts, determine what's critical, prioritize which alerts to respond to, and take the right action. At this point, the law of diminishing returns starts to come into effect.

It is virtually impossible for overstretched and understaffed SOCs to review all the alerts, determine what's critical, prioritize which alerts to respond to, and take the right action.

The reality is, while a layered defense is a critical component of a sound security strategy, It is still not enough to keep you safe. You can't get the context you need to take the right action fast enough or know if a threat is real, how it might behave in your environment, and how it will put your business at risk.

In fact, the only way to get the context you need to fight your adversaries is to execute your security plan in a way that allows you to coordinate across all your layers of defense with the right technology, human intelligence, and processes working together - in concert.

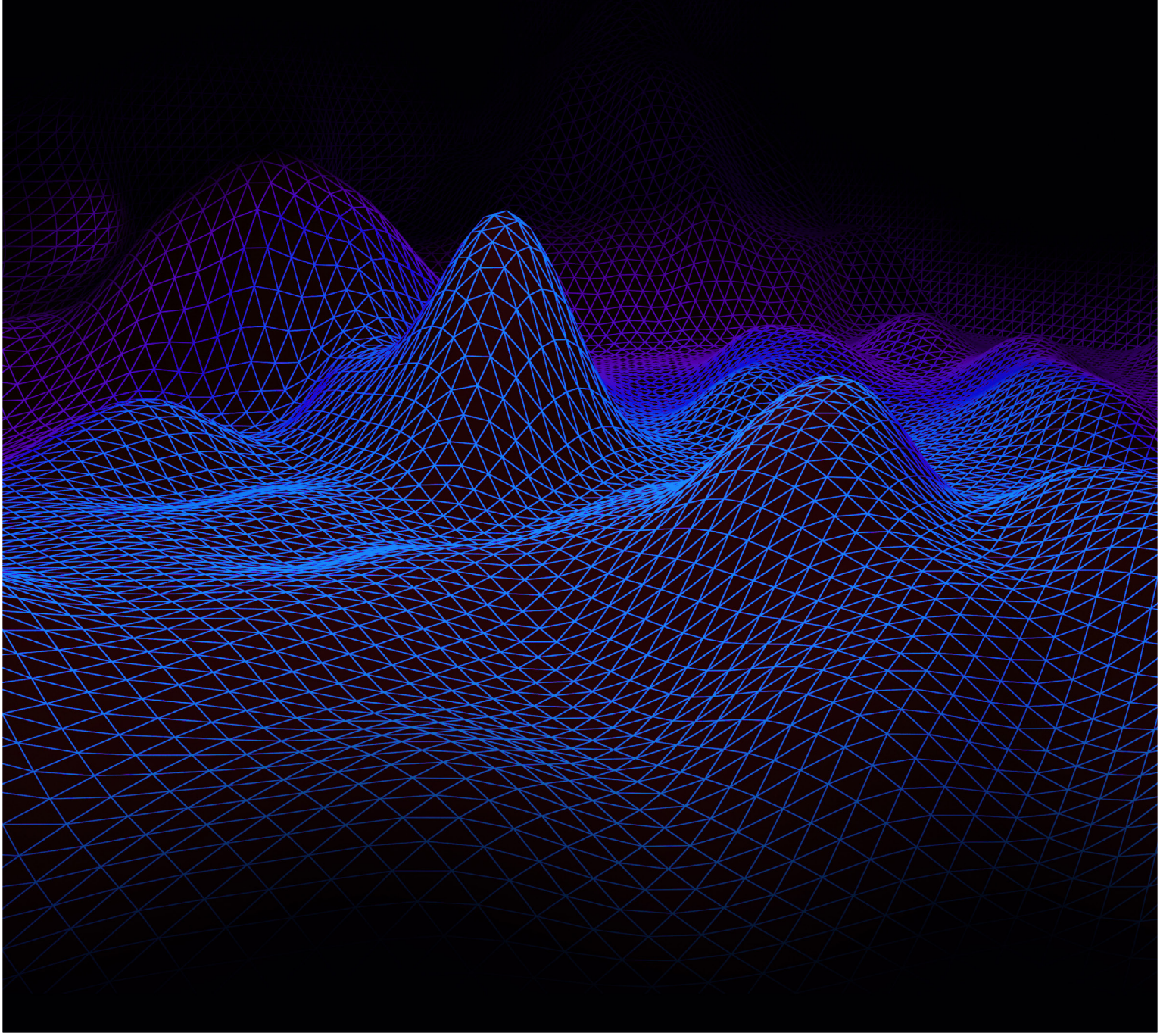
After execution, you should be able to:

- Assess, design, and test your defenses
- Seal the gaps in both your technology and security hygiene
- Anticipate and respond to evolving threat actor behaviors—their ever-changing tactics, techniques, and procedures, as well as their motives and the ramifications they could have on your business

Then you can be satisfied that you've created and executed a plan that has moved you to a more mature security posture. At the end of the day, what most companies need to reduce their risk isn't just more technology. What they need is a coordinated approach across all the layers to reduce inefficiency and complexity, make better use of investments, and reduce risk exposure.

However, for true security maturity, you aren't finished yet.

The world of IT is becoming ever more complex at the same time as threats are multiplying. That means instead of viewing security maturity as a one-time goal, you should be continually striving to move your security along the maturity axis.



FOUR

Continue to Evolve - Along the Maturity Axis

Just as cybercriminals continually evolve their methods of attack, so does the secure organization need to evolve its security posture. The world of IT is becoming ever more complex at the same time as threats are multiplying. That means instead of viewing security maturity as a one-time goal, you should be continually striving to move your security along the maturity axis.

It is Secureworks' opinion that organizations are found in one of four maturity tiers:

Guarded: These organizations implement basic network protection often using off-the-shelf tools and technology with limited customization and a focus on compliance. The security team is typically embedded within the overall IT organization with split responsibility between IT and Security and managed by mid-level managers. These organizations tend to not have CISO-level leadership. Cloud solutions are often run independent of the security team.

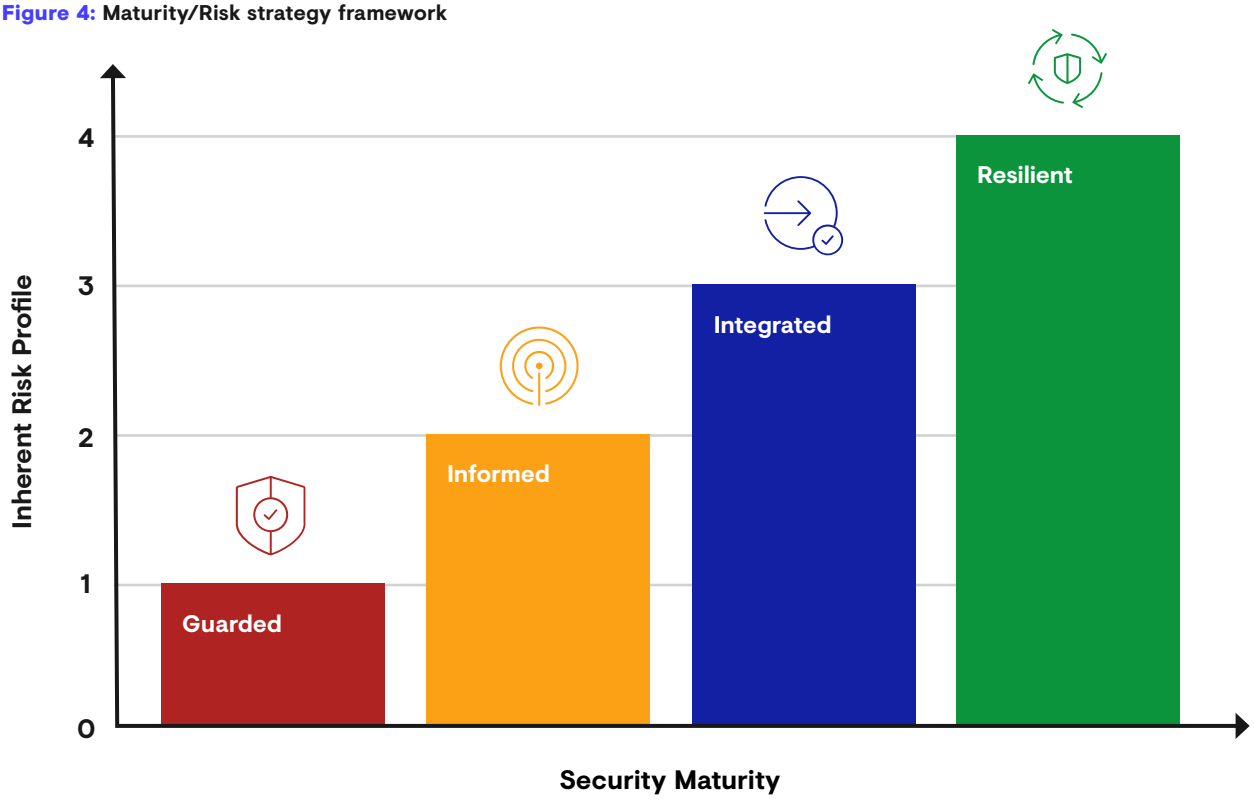
Informed: These organizations often have security teams with their own senior leadership and reporting structures yet still fall under the overall IT department. The security teams have started to standardize IR procedures and, operationally, integrate multiple TI sources. They tend to implement more layered defence tactics and leverage more Security technology. They also extend their influence into the business with more input, but still limited control over Cloud services.

Integrated: These organizations approach security with a proactive face often customizing and extending their IR, endpoint and TI capabilities into the company operations. Their security teams are larger and have more resources available to manage advanced security operations, augmenting their in-house capability with third parties to give better coverage across the business. The security leader, often a C-level executive, applies security thinking to business strategy and operations planning.

Resilient: These organizations standardize and embed security activities within and across business operations, enabling them to withstand or recover quickly from security issues. These organizations have larger inherent risk due to the nature of their business and integrate advanced techniques like AI and ML into the security infrastructure. The business, as a whole, is engaged in security planning and execution. Given the level of expertise, these organizations typically have large internal staffs and a C-level CISO who provides regular Board-level reports on security matters.

Figure 4 below provides a visual of these four stages and the relationship between maturity and an organizations inherent risk.

Figure 4: **Maturity/Risk strategy framework**



Not all organizations need to reach a Resilient maturity tier. There are a number of factors that drive the target maturity, defined in our Inherent Risk Profile. These include elements such as:

- The organization's industry
- Number of employees
- Type of information assets the organization processes
- Volume of information assets
- Services offered by the organization

To be able to progress along this axis, you need to be able to assess and demonstrate the effectiveness of the program you've put in place. That's important for judging progress and for maintaining continued executive buy-in. A major concept for measuring success in cybersecurity terms is resilience. That means how effectively and efficiently the organization finds and removes threats from its environment and how effectively it continues to conduct business while doing so. And that requires the capabilities for early warning and early intervention.

This paper has already discussed how compliance is not the same as security. Clearly then, measuring compliance is not the same as measuring resilience. It can be useful to benchmark against external security measures. For example, Secureworks has developed the Secureworks Security Maturity Model, which allows organizations to quantitatively assess themselves against external benchmarks across five (5) security-specific domains:

- Security Organization and Governance
- Security Operations
- Cloud Security
- Incidence Management
- Threat Intelligence

Our model is also valuable for conducting real world exercises to battle test one's own environment. Details about the complimentary Security Maturity evaluation with Secureworks can be found at the end of this paper or here (www.secureworks.com/resources/wp-secureworks-security-maturity-model).

It is important to establish a consistent set of metrics, particularly when it comes to reporting performance to the Board. These metrics can be organized into a dashboard to aid accessibility.

Less is more on your dashboard and the business relevance and quality of your metrics are more important than volume. Rather than presenting the number of unpatched systems, for example, provide a month-over-month update on patch latency, specifically for mission-critical systems. Within the dashboard, key metrics should be replicable—appearing consistently in each report over time—to help Board members assess risk trends and improvement in resilience over time. Insights from the metrics can be used to highlight how security is supporting the organization's key strategic initiatives.

The following list provides examples of metrics that could be used for reporting:

- Emerging threat trends
- Incident or breach trends
- Time to respond
- Time to detect
- Vulnerability management
- Compliance and control
- Regular reporting on the organizations maturity score
- Data loss prevention, integrity, and availability
- Third party vendor risk
- Employee awareness
- Status of key initiatives
- Assessment results

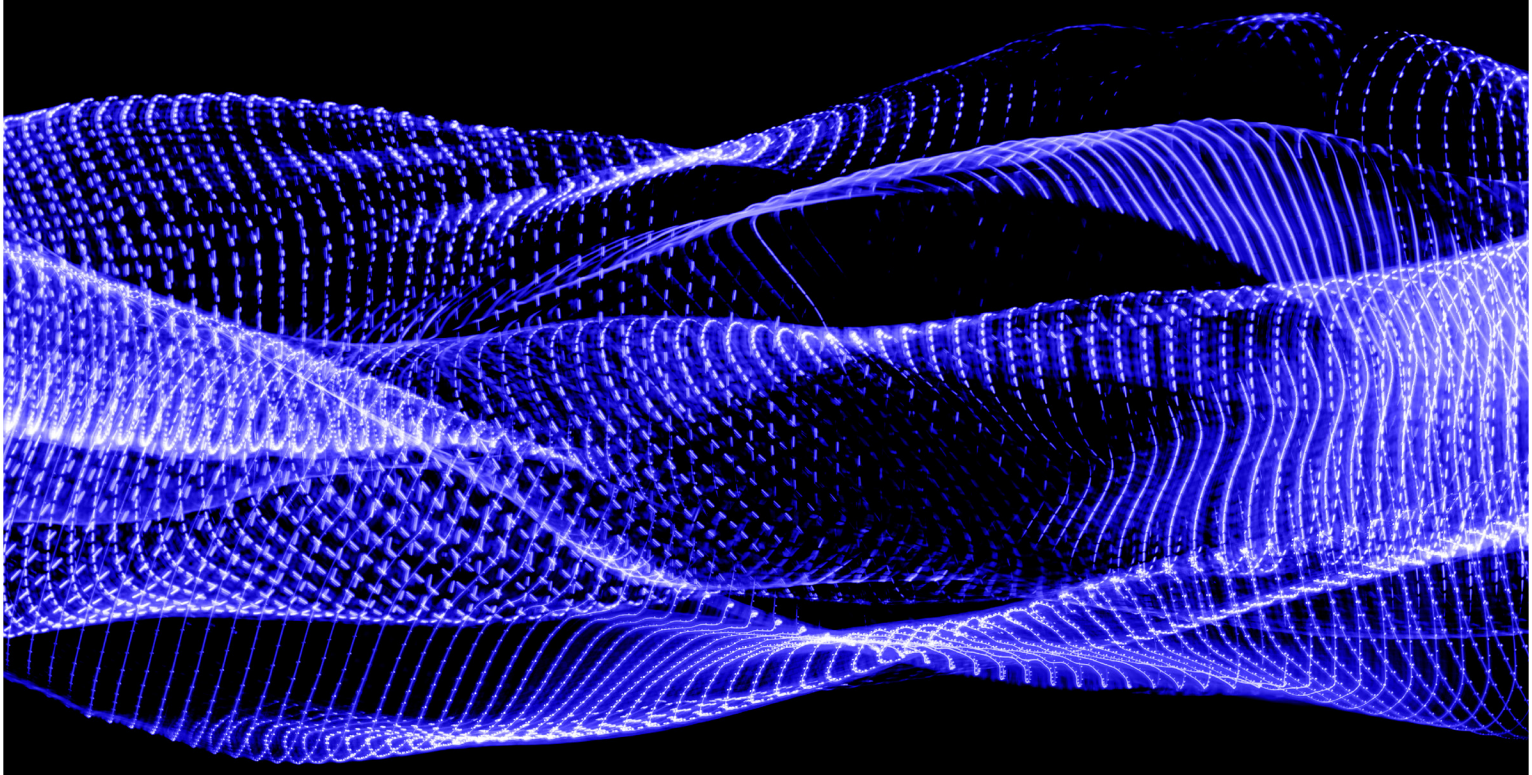
As we discussed in the previous section, security maturity does not come from purchasing every new piece of technology that comes to market. What is important however is investing in resource – for many organizations one of the biggest enhancements would be to ensure that you have trained, capable analyst cover consistently available in your SOC. Cyber-criminals don't just work standard business hours – nor should your security resources.

So, as an organization's security maturity increases, it becomes less purely reactive, more proactive and more resilient as it moves to a point where it can continuously address risks in real time. As risk is reduced, so is cost. In addition, when you invest in predictive capabilities, as well as continuous validation and assessment of real risk, you gain efficiency, and as a result you spend only on the threats that matter most.

Even more importantly for budget authorities and CFOs: when you become more predictive about the threats, you become more predictive about risk and spend. You therefore can grow and transform with greater confidence.

Maturity is about making security solutions, people and process work for the business, not just for security. Increased efficiency and effectiveness helps close the gap between security investments you're making now, and desired business outcomes.

Through devising and executing a risk-based security plan, you've already made major strides towards security maturity. To maintain this, you need to future proof.



FIVE

Future Proofing – Through Creating a Culture of Security

Through devising and executing a risk-based security plan, you've already made major strides towards security maturity. To maintain this, you need to future proof. The way to do that is through creating a culture of security in your organization that continually considers the digital transformation that is taking place today.

There are five key features of cybersecurity culture:

- Communication frameworks
- Shifting security away from being an IT-only issue to a business operations issue
- Building everything an organization does with security in mind
- Demonstrating value
- Changing the face of end user awareness that embraces cybersecurity and provides a message that supports and rewards positive cybersecurity behavior

Creating Effective Communications

Creating a culture of security requires effective communications across the enterprise. Security is the responsibility of all levels of the corporate hierarchy. The Board is responsible to the company's shareowners and stakeholders for cybersecurity risk oversight. Board members will need to understand the nature and severity of the risks to weigh in on the risk appetite for the assets at stake. This will allow them to sign off on decisions involving the budget or strategic impact on the company.

Figure 5: Executive/board oversight of cybersecurity maturity

The CEO and Executive Management team are responsible for risk management, which involves enforcing the policies and procedures that support the cybersecurity program. These responsibilities include funding the program adequately, monitoring the risks and ensuring the company is responding accordingly when the threat landscape changes or a crisis occurs.

The Senior Leadership team, the Incident Response team, Legal, PR, the InfoSec team, lines-of-business leaders and employees all have distinct roles in protecting the enterprise and minimizing damage if a breach does occur. And that's just the internal communications. External communications with the public, customers, regulators, shareholders and law enforcement must also come into the mix. This very complexity trumpets the need for clearly defining the roles and responsibilities of all involved and developing a communications flow among them. The below is a good example of a comprehensive framework but it is necessary that adjustments are made to suit your organization based on your business size, organizational structure, and departmental dependencies.

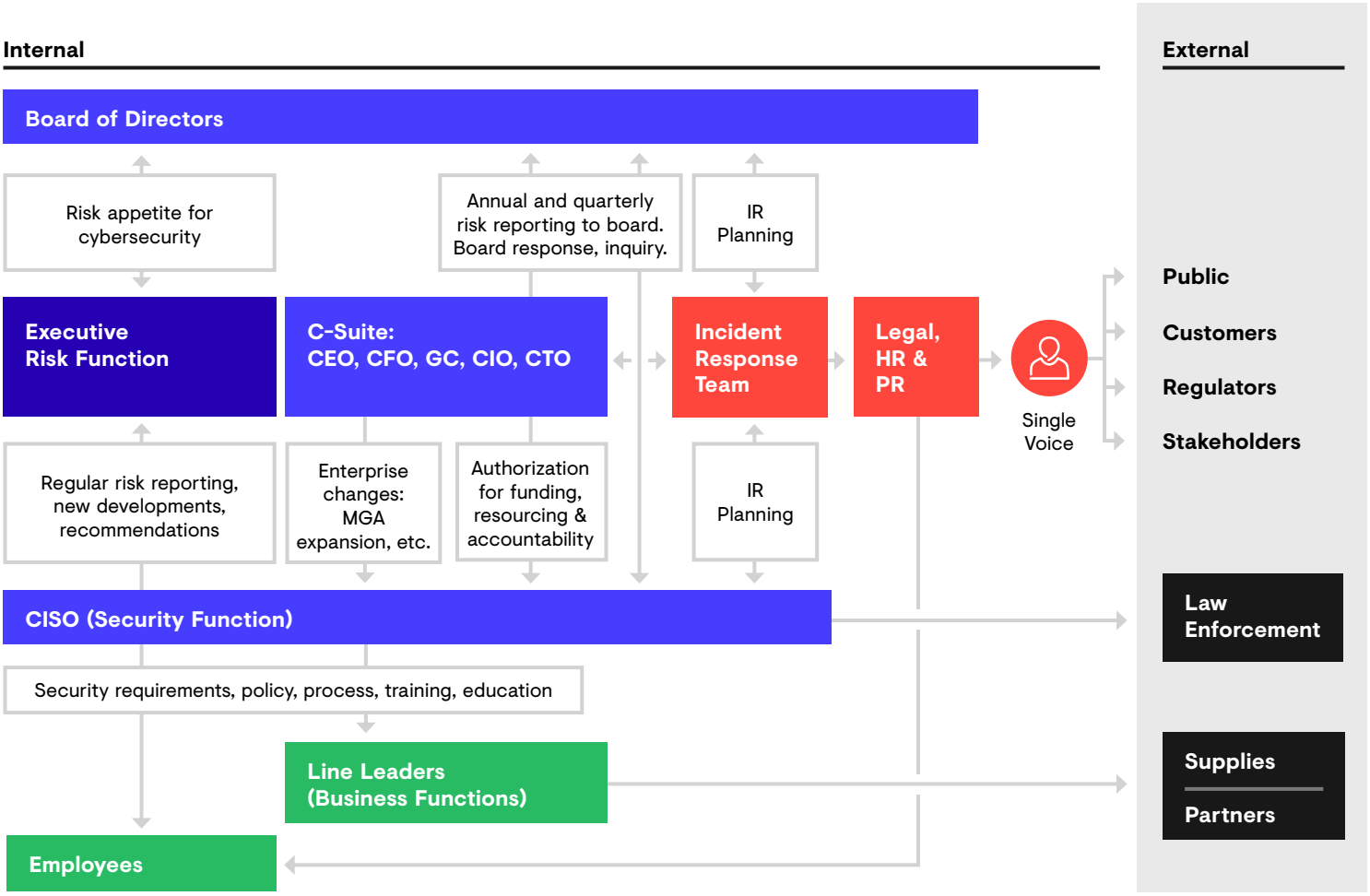


Figure 6: Security program communications

It is critical that the executive risk function vets the overall risk plan with business stakeholders, including the CIO, HR, Legal and Compliance, and considers law enforcement ramifications to ensure consensus before taking the plan back to the Board. It is a closed-loop that leaves no gaps. Legal also plays a key role, particularly if there is a breach. Legal decides if the Board (or law enforcement, or the public) gets notified. If so, the Board has direct responsibility and works with Legal to figure out who will communicate about the breach, and to whom, with one single voice.

For true security maturity, cybersecurity must move from the IT realm to that of business operations.

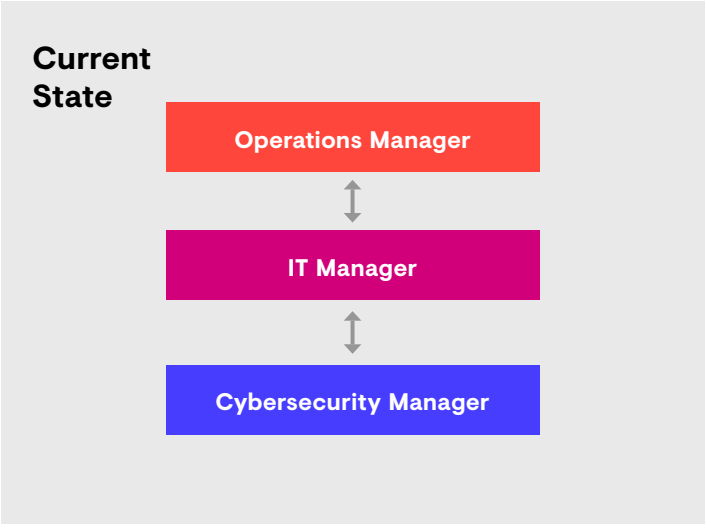
For example:

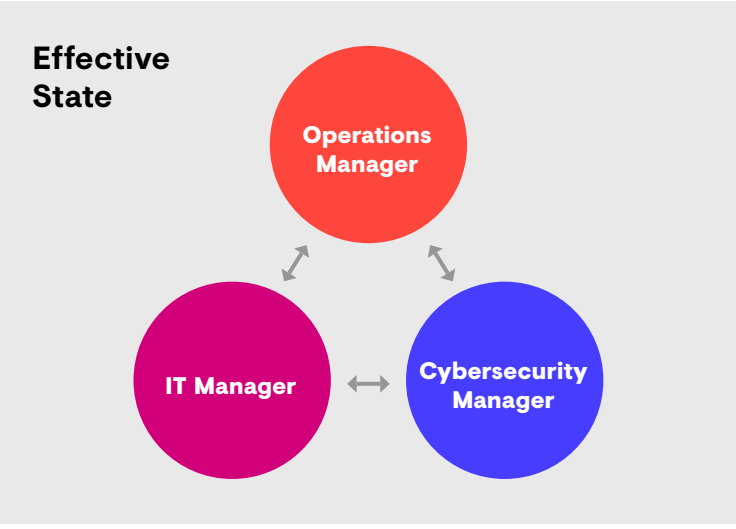
- Public Relations works with the press
- Legal works with regulators
- The security leader works with law enforcement under the guidance of Legal
- General Counsel takes the lead in filtering communications to mitigate risk, ensuring that employees, customers, suppliers and partners receive appropriate information and align with legal obligations

Ultimately, ensuring a closed-loop communications flow mitigates the risk of breakdowns that lead to reputation damage. The right people disseminate the right information, customers are appropriately notified, and companies can mitigate further harm to the brand and stay on the right side of regulators.

Incorporate Security Into Business Operations

Today, cybersecurity tends to fall under information technology management. Often the cybersecurity leader reports to the CIO or one of their direct reports. This is understandable since the need for cybersecurity arises from the ever-changing information technology landscape. The more technology plays a role in how business is done in this world, the more cybersecurity becomes an issue.





For true security maturity, cybersecurity must move from the IT realm to that of business operations. Chief Operating Officers are often confronted with situations that have security implications; for example, perhaps a department is looking to leverage cloud services to set up a pilot for a new product. Understanding the impact that cloud services might have on an organization's security strategy is key to preventing an additional layer of risk to the business. Cybersecurity managers need to be able to represent security considerations to a decision maker who is not conflicted by their main role in running IT. Someone like the COO who has the breadth of responsibility is ultimately more likely to be able to make those decisions with business interests in mind.

This means IT management can focus on what they do best, which is leverage technology to provide world-class services to an organization, while the operations side of the business works closely with IT management and security management to ensure that the service being produced does not add layers of unmanageable risk to the business.

Build With Security in Mind

Everything an organization does should be built with security in mind. Yet few developers have security as a priority. We have seen, time and time again, amazing software developed that can be a game changer for organizations, and yet this software has looming zero-day vulnerabilities. We have done multiple web application test engagements that have highlighted issues with code that require a complete rewrite of the software. All that could have been avoided if Development Operations had done source code analysis for these vulnerabilities and patched them as the code was being developed.

Another example involves marketing departments that purchase third-party technology to support their efforts and gain market advantage over competitors. They do this without thinking about potential consequences, such as what data that third-party technology will need access to, or how the technology works, or the attack surface it possibly opens to increased potential business risk.

If organizations can create and implement an organizational-wide shift in mentality that encourages 'build with security in mind', then the benefits will be far reaching. This shift requires a lot of time and work for an organization to see the net effect, but the return on investment is well worth it. To make this happen, organizations must change their attitude to end user training and awareness.

End User Awareness in a Whole New Light

In the past, organizations have typically dealt with end user security awareness by testing users with simulated phishing emails and punishing those who fail. Yet it is known that negative punishment is a poor choice for changing behavior and rewarding positive behaviors is more effective.

Alternative approaches could include:

- Security promotion posters that give quick nuggets of security information to serve as constant reminders to end users
- Personal security assessments to help individuals identify their own gaps in their personal cybersecurity. This might include testing them against the number of passwords they have, how many websites they use the same password for, and whether their passwords use capital and lowercase letters that include special characters and numeric keys
- Monthly security champion rewards for people who show exceptional cybersecurity savviness such as reporting scam emails, having good password hygiene or identifying things they think might cause risk to a business
- Departmental security champions who are going to be the voice for cybersecurity. Meet with them monthly and share knowledge, determine what the organization needs to do better and promote the monthly security champions award in their own department
- Monthly cybersecurity tips and tricks newsletter for users, which can be used as a way for a business to make people aware of common scams that are going around, promote free services such as www.haveibeenpowned.com and share current news about national and international cybersecurity

Conclusion

Change is never easy, but it is necessary. Organizations that want to future proof their cybersecurity strategy and reduce business risk need to ensure they close the loop by fostering an organizational-wide culture that embraces cybersecurity. This may help any organization to future proof its security strategy by making security a focal point of everything it does, ensuring that it walks side by side with an organization's digital transformation.

The strategies and tactics described in this paper may help create a coordinated, intelligence-driven defense that reduces risk by making you more able to more accurately predict when and where attacks may happen and better equipped to prevent more breaches from taking place. You may also be able to detect malicious activity faster, have the context to quickly prioritize the threats that carry real risk, and respond with the right action—the one that protects you best—sooner.

Finally, you may reduce complexity in your security infrastructure and get more value from your security resources and spend. And most importantly, you'll have changed security from a business inhibitor to a business enabler, empowering your business to evolve and grow.

For all organizations though, there will always be some aspects of security that will be harder to transform than others. That's when working with a trusted security partner can really pay dividends.

Click below to request a Secureworks Security Maturity Evaluation or click here to learn more about how the Security Maturity Model can help your organization. Or call your regional security expert using the phone numbers located on the back page.

Request a Secureworks Security Maturity Evaluation

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500 Atlanta,
GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp