SECURITY FRAMEWORK: A GUIDE FOR BUSINESS LEADERS

Executive Summary

While few corporate executives and boards of directors would dispute the importance of cybersecurity, some may feel ill-prepared to begin the process of managing these risks given the myriad technical and non-technical elements of the issue. The goal of this document is to address this gap by providing corporate leaders a practical framework for addressing the people, process, and technology elements of the cybersecurity challenge.

Although information technology has created a new digital age, transforming every aspect of modern life and bringing with it greatly enhanced productivity gains and standards of living, its underlying infrastructure is inherently vulnerable to exploitation. This leaves society open to fundamental cybersecurity risks. Businesses globally constantly face an onslaught of malicious activity, ranging from theft of precious intellectual property and customer records to destruction of valuable proprietary information.

While there are significant financial costs to these incidents, the cumulative effect of the increasing torrent of cyberattacks is an erosion of the trust that enables our digital age. The fine line between a high functioning digital society and the collapsed productivity that would transpire in the absence of such trust defines the cybersecurity imperative for leaders in all sectors, particularly business executives. Businesses own and operate the assets that enable our digital society, and therefore have a fundamental interest in managing the cybersecurity risks facing their companies.

Although the volume of cybersecurity-related news has generated awareness of the topic, it has also sowed confusion, fear, uncertainty, and doubt (FUD) about the key issues business leaders need to consider. It is important, therefore, to define the problem that needs to be addressed.

In its simplest terms, the current cybersecurity challenge is a competitive strategy and risk management situation familiar to many. Thanks to the technological advances that have greatly increased access to computing power and the ability for on-line collaboration and information sharing, attackers enjoy decreasing start-up and marginal costs. This has led to a dramatic increase in both the volume and sophistication of the attacks they can launch. Defenders, consequently, face increasing fixed and marginal costs while investing in the personnel and technology necessary to confront the attacking onslaught. The frequent headlines announcing yet another successful attack are the predictable results of this asymmetric conflict.

Current approaches to cybersecurity, which focus on detection and remediation, are inadequate to deal sufficiently with the rise in volume and sophistication of attacks. In basic terms, the difference between an attacker launching 10 or 10,000 attacks against a corporate network is a marginal investment of time and computing power. Defenders, meanwhile, given the current security technology paradigm, would need to scale with individuals to detect and respond to an equivalent 1000x increase in activity. In other words, attackers scale with technology and defenders scale with humans. Additionally, organizations increasingly face targeted attacks, encountering never-before-seen malware while relying on a patchwork of technologies that do not integrate to prevent malicious activity.

Since corporations are ill-positioned to change elements of this imbalance, such as certain political environments that permit and facilitate cybercrime and cyberespionage, the fundamental goal of any corporate cybersecurity program should therefore be to prevent cyberattacks to a degree that changes the economics of this dynamic to make it making it more difficult, i.e., less profitable and less attractive, to execute a successful attack. In addition, a focus on resilience is critical so that firms can limit the damage of successful attacks and recover quickly.

Given the technological and economic dynamics that greatly favor attackers, defenders must adopt a new approach to counter malicious actors and to prevent successful attacks—the loss of the confidentiality, integrity, or availability of corporate assets. This fundamental shift starts with the identification of the firm's most critical assets and a thorough risk assessment of the potential threats and vulnerabilities impacting those critical assets. Once this risk analysis is complete, firms can focus on automating the manual activities of detection and remediation to an adaptive, repeatable process that prevents breaches and achieves meaningful security that changes the economics of cyberattacks target the firm's most critical assets.

To appropriately manage the risk of cyberattacks and to prevent successful attacks, businesses must structure their cybersecurity programs to:

1. **Identify** organization-specific critical assets, priorities and related governance structures;
2. **Monitor and analyze** all traffic to establish visibility of all users, applications, and content traversing corporate networks, clouds, and endpoints, in order to define and refine organizational information security policies;
3. **Protect** from attack by enforcing policy to reduce organizational attack surface, **and prevent** known and unknown threats; and
4. **Detect and respond** to the inevitable successful attack in a manner that incorporates mitigations and protection mechanisms to prevent similar attacks in the future.

While this approach draws on the NIST Cybersecurity Framework, the sequencing of some activities is intentionally different. A fundamental shortcoming with many current approaches to managing cybersecurity risk that this framework seeks to remedy is a lack of full visibility of users, applications, and content traversing corporate networks, cloud, and endpoints. This by definition limits the effectiveness of protection efforts, as an organization cannot protect against what it does not observe. With this full visibility, organizations will be empowered to implement security policies oriented to prevent attacks firstly, thereby enhancing organizational effectiveness at detecting and responding to a more limited set of attacks that may still be successful.

While there does not yet exist the equivalent of mean-variance analysis to guide cybersecurity investments, executives should allocate resources to enable the adoption of the aforementioned four-part structure in order to optimize organizational agility and efficiency while minimizing cyber risk. While risk appetites will necessarily differ between companies and industries, the overarching philosophy of making cybersecurity investments to securely enable productivity will not.

Table of Contents

Identify: Setting Organizational Priorities

Given the fundamental reliance of businesses on properly functioning technology to generate enterprise value, cybersecurity must be an enabling function rather than a control function. Cybersecurity practices to date have existed in the domain of controls and compliance, which has led to friction between the business and security teams at organizations across industries and sectors. Determining the corporate approach to cybersecurity must therefore be an executive-level, cross-functional, and risk-based discussion to identify fundamental business priorities and requirements as a point of departure.

Determine Business Priorities and Requirements

In order to structure an effective cybersecurity program, organizations must determine what to protect in order to securely enable operations.

1. This begins with identifying the strategic priorities of the organization, as well as the supporting revenue streams, critical data, key business functions, applications, and dependencies.
2. After these are identified, businesses must understand where they are located, who has access to them today and who should have access to them. Based on this understanding, organizations must establish priorities for resilience and determine organizational cybersecurity risk tolerance.
3. Because of the fundamental importance of cybersecurity to organizations, this must be a cross-functional, executive-level process, which will inform the subsequent establishment of cybersecurity processes and guide technology investment.

Key steps	Key considerations
Identify critical assets and important business processes	• Complete a combination manual and automated data discovery and tagging program to identify organizational critical data or "crown jewels." • Crown jewels are those information assets or processes, which if stolen, compromised, or used inappropriately would render significant hardship to the business. • Examples of crown jewels may include trade secrets, market-based strategies, proprietary algorithms, product designs, new market plans, regulated personal data and data security practices, or other business processes in addition to information assets.
Determine value of each asset and business process to the organization	• A "one-size-fits-all" model doesn't apply when protecting key information even to a particular data asset within an organization, since certain data elements may have a different criticality to different business units, requiring different levels of protection. • Organizations should hold business executives accountable for protecting the crown jewels in the same manner as they are accountable for financial results.
Define risk tolerance levels	• Organizations should define the right level of risk tolerance for their organization based on their business type and regulatory obligations. This will help determine the level of protection needed given their identified values and related risks.
Establish the levels of protection required for each asset type	• This would also include defining the ownership of risk for each asset, and establishing who within the organization can make decisions on accepting or mitigating risks related to them. • Organizations can then prioritize their assets based on business risk.

Establish Policy and Governance Structures

Similar to the determination of priorities and requirements, organizations must also establish policy and governance structures to facilitate oversight and accountability for cybersecurity. While the specifics of such structures will necessarily differ to account for organizational specifics, obtaining cross-functional, executive-level engagement will be crucial to establish that all implicated stakeholders take ownership of their cybersecurity responsibilities.

1. Specifically, organizations must establish and communicate security roles and responsibilities for the board of directors, executive management, and the workforce.
2. Additionally, organizations must understand their legal and regulatory requirements related to cybersecurity and data governance to inform, but not dictate, their approach. While it is now well-established that compliance does not necessarily result in security, effective cybersecurity practices are fundamental to many compliance responses and may help to mitigate enforcement actions in the event of a violation.
3. Finally, organizations must align corporate governance processes to account for cybersecurity risk; for example, by tasking an existing subcommittee of the board of director's audit committee or a cross-functional executive team.

The foundation of a strong cyber-resilient organization is a sustainable governance process for managing cyber risks. To be sustainable, the governance process must enable access for key stakeholders. Deciding which business and teams need to be on each of the teams will depend on the particular business model and market of the organization. Depending on the size and complexity of an organization, multiple governance committees may be required to cascade responsibilities and to monitor activities. Operating processes for each and a reporting structure are needed to facilitate consistent information flow and risk monitoring.

Typically, three groups should be organized to carry out these efforts if these responsibilities aren't already assigned to existing groups. Specific membership may differ or interchange depending on organizational needs, core activities, and changes in risk profile. Organizations should seek to integrate these responsibilities with existing groups or committees, wherever appropriate, to avoid committee or council fatigue and the dilution in value of respective forums.

Group	Key players	Responsibilities
Cyber risk governance committee	• Chief Operating Officer (COO) • General Counsel (GC) • Chief Risk Officer (CRO) or Chief Audit Officer (GA) • Head of security • Heads of businesses and functional areas (such as business continuity planning, legal, compliance)	• Works with senior leaders to develop cyber risk strategy. • Confirms which information assets are essential. • Sets the budget for cyber risk. • Identifies and validates legal and regulatory obligations. • Monitors the organization's cyber risk position and reports on it to senior leaders and the board of directors. • Reviews reports from the cyber risk oversight and operations teams and helps prioritize emerging cyberthreats. • Revisits strategy to adapt the program as the cyber risk landscape evolves.
Cyber risk oversight committee	• Information technology team • Business operations support team leaders • Critical business team leaders incl. HR • Chief Information Security Officer (CISO) • Chief Privacy Officer (CPO) or equivalent	• Assesses the active risks the organization faces, the people behind them, and the assets they threaten. • Evaluates the effectiveness of the operations team. • Consolidates operations team report and prioritizes information and technical asset importance to the governance committee • Identifies new threats and improves how information assets are protected. • Determines how business changes affect the cyber perimeter — including new service offerings, suppliers, vendors, and business partners. • Monitors status of patches and configuration changes to critical systems. • Oversees employee training programs. • Reviews new regulatory and compliance requirements.
Cyber risk operations team	• Managers with operational experience of networks, information security, fraud, and corporate security • Security operations center	• Acts as first line of defense for detecting and responding to cyber events. • Compiles real-time information from all the groups that monitor cyberthreats. • Produces reports for the cyber risk oversight and governance committees, including items such as: number and type of cyber events, origination and duration of events, which assets have been targeted, kinds of fraud attempted, comparison of cyber events to industry trends, incident and response reports, threat assessments, and intelligence reports.

In highly diverse or federated organizations, there may be multiple operations teams supporting the oversight committee.

Implement Hardware and Software Asset Management

To assist with the scoping of cybersecurity risk tolerance and management, organizations must implement continuous and automated asset management. This allows for the identification and classification of all enterprise hardware, software, and critical or high-risk data, cataloging of external information storage and processing conducted by partners and other third parties, and mapping of organizational data flows. The outputs of these efforts will form the basis of risk management discussions, as they will provide necessary contextual information for decision-makers.

Develop Risk Management Strategy

Cybersecurity is an enterprise risk, and organizations must therefore incorporate it into preexisting risk management structures or establish new ones as necessary. Here again, having cross-functional executive-level engagement will be important to identify key technical risks and their business impacts, as well as to assess the productivity versus risk implications of security controls for information assets. Crucially, organizations will need to ensure that their cybersecurity governance structures are adequately aligned to meet their risk management goals; organizations should manage security risk by design and default.

Key steps	Key considerations
Bring together the various teams responsible for managing, tracking, and responding to cyber events	This should include the following: • Internal security operations center (SOC): IT operations team, systems for security information and event management (SIEM), and incident-response teams. • Cyber risk governance: cyber risk governance committee, cyber risk oversight committee, and cyber risk operations team. • Cyberthreat intelligence can also provide valuable information to groups responsible for detecting identify theft, fraud, money laundering, and terrorism financing.
Adjust cyber risk and control posture of the organization	• Adjust approach and segmentation as needed, depending on the location of assets, threat incidence, and state-of-the-industry landscape. • Refine and update processes, as necessary, to adjust to evolving cyber risk landscape.

Monitor and Analyze: Full Visibility of Network, Endpoints, Cloud and SaaS

In order to prevent attacks, organizations must have visibility into all the internal and external data transiting their environments, an increasingly challenging imperative given enterprise technology trends, such as mobility and the adoption of cloud computing and Software as a Service (SaaS). Strong monitoring and analysis capabilities are therefore a key component of a prevention-oriented approach to cybersecurity. Analyzing the data collected from network, endpoint, application, data, cloud, and SaaS environments gives a full contextual view of activity, which can then be interpreted to enable protection and prevention actions.

Observe All Network Traffic

There are three imperatives to establishing visibility over all network traffic to gain the contextual view necessary to prevent attacks:

1. First, monitor and log all traffic of all internal network segmentations and network egress points. Such monitoring enables the detection, and subsequent prevention, of malicious activity once an adversary has breached an organizational perimeter.
2. Second, monitor and log all network traffic of all users, both on- and off-premise. By monitoring the traffic of all users, organizations eliminate visibility gaps, further providing the full context needed to enforce security policy.
3. Finally, organizations must monitor and log all network traffic accessing corporate cloud and SaaS resources. Without visibility into how data is accessed, regardless of where that data resides, organizations will not be in a position to prevent data compromise.

Establish Visibility of All Applications, Users, and Content Traversing Network

Although observing all network traffic is a necessary component of establishing an effective cyberattack prevention capability, it must be properly contextualized with mapping to specific application usage and user identities to enable the enforcement of application-, user-, and content-based security policy. Additionally, organizations must have the capability to decrypt encrypted inbound and outbound data flows to facilitate full visibility into the network traffic of select applications, as adversaries increasingly use encrypted channels to exfiltrate data. This full context is of utmost importance and is what enables companies to set risk-based security policy. Finally, organizations must manage the identities and credentials for authorized devices and users to prevent the use of stolen equipment or compromised credentials for malicious purposes.

Define and/or Refine Organizational Information Security and Technology Acceptable Use Policies

Armed with the data of full contextual monitoring and analysis of network traffic, organizations can decide which critical applications they wish to allow to support business operations, which to deny by default, and what level of further analysis to apply to unknown traffic. Determining how to classify the applications running in a corporate environment requires, again, cross-functional, executive-level input and should be done with input from senior management and technical staff. This process will allow for the automatic enforcement of application-, user-, and content-based security and technology acceptable use policies grounded in fully observed network traffic. In addition, once such policies are established, organizations must implement cybersecurity awareness training in order to further develop employee sensitivity to security and instill a culture of shared responsibility for safeguarding corporate data.

Protect and Prevent: Visibility and Context-Enabled Cyberattack Prevention

Having a full, contextual inventory of the network, endpoint, cloud, and SaaS environments enables the implementation of a positive enforcement security policy that enables sanctioned activity, denies the unsanctioned, and subjects unknown activity to further scrutiny. In turn, this allows for systematic management of the unknown, reducing organizational cybersecurity risk.

Develop and Enforce Technical Policies to Reduce Attack Surface

While contextual data allows organizations to determine information security and technology acceptable use processes and policies, these must be implemented through technology. Technologies categories, such as Vulnerability Management, Network and Infrastructure, Endpoint, Message, Application and Data Security, can all reduce the attack surface area. This will allow organizations to reduce their attack surface, or security risk liability. Attack surface reduction is achieved by three actions:

1. First, implement an application whitelist – enabling critical business applications and denying all others by default.
2. Second, inspect and judge unknown traffic and activity against previously determined information security and acceptable use policies to determine whether or not to allow it to execute.
3. Finally, enforce role-based access to applications and data content where possible to ensure that compromised credentials cannot be used to access applications and data. This is critical to ensure that only the appropriate users have access to the applications and data necessary for them to complete their jobs, while limiting the potential damage an attacker can inflict with compromised credentials.

Prevent Known Threats

Preventing known threats is a foundational capability of any security program; but, in order to do so effectively, organizations must be able to consume and process threat intelligence and have well-organized defenses that can be reconfigured automatically based upon new intelligence:

1. Establish a logical security perimeter not bound to the physical or logical location of devices or data. This means that organizational data flow is protected regardless of whether it is accessed on- or off-premise, according to policy.
2. Block known threats with existing controls and intelligence.
3. Integrate cloud access security with threat detection. Data resident within enterprise-enabled SaaS applications is not visible to an organization's network perimeter. Adding the ability to connect directly to enterprise SaaS applications to provide data classification, sharing visibility, and threat detection within the application enables organizations to inspect content for data risk violations and control access to shared data with a contextual policy.
4. Match newly created controls to block previously unknown malicious payloads.
5. Automate reprogramming of all security technologies to incorporate these new controls.

Prevent Unknown Threats

Although preventing known threats is vitally important, signature-based prevention is limited, by definition, to block only what it knows to block. Unfortunately, given the rapid pace of change in attacks, relying on preventing known threats alone consigns organizations to a reactive security posture in which they will always be at least one step behind adversaries. Preventing unknown threats is, therefore, a crucial capability, and essentially consists of the process of making unknown threats known, developing controls to stop them, and automatically reprogramming security technologies to incorporate the new controls. Accomplishing this requires four main activities:

1. Protect endpoints with technology that prevents exploit and malware techniques. Instead of the reactive posture of keeping pace with the millions of new signatures, it is more efficient and effective to block the dozens of known exploit and malware techniques uniquely associated with malicious activity.
2. Identify and block malicious lateral movement between network, endpoint, cloud, and SaaS environments. In this case, even if an adversary breaches the perimeter, the threat can be prevented before an attack is successful.
3. Incorporate external threat intelligence sources to security monitoring. No organization will have full knowledge of the threat environment, but being part of a threat intelligence community enables the creation of a strong network effect to counter the emergence of new threats.
4. Automate analysis of external threat intelligence sources. Threat intelligence data is only useful insofar as it assists in preventing attacks. Organizations should deploy technology that automates the analysis of external threat intelligence to provide prioritized, actionable intelligence on the attacks that demand response, with the context to take immediate action.

Detect and Respond: Rapidly Mitigate and Automate Protection

While organizations should adopt a prevention-oriented approach to cybersecurity, it is unrealistic to believe that all attacks will be prevented or detected in a timely manner; and organizations must, therefore, be prepared for incident response, ensuring that the technical and procedural lessons learned are inculcated to prevent similar incidents in the future.

Establish, Test, and Execute Incident Response Plan

Since cybersecurity is an enterprise risk, organizations must establish and conduct regular tests of incident response and recovery plans with the executive staff, technical teams, and key external specialist teams, such as legal, communications, and forensic professionals; an organization's first cybersecurity crisis should not be a live one. Incident response plans should include guidelines for when to trigger response and recovery plans, and when to engage external parties; and they should be executed according to these guidelines. Upon completion of the incident, there should be a cross-functional, executive-level, after-action review to refine the organizational response and recovery plan.

Key steps	Key considerations
Devise scenarios	• Think about the biggest cyber risks to your business and develop scenarios for some of the ways in which they're likely to happen. Each scenario should focus on a particular type of cyberattack and the assets it threatens. The scenario should also include the effects on your reputation, customers, finances, and your position with regulators.
Mitigate the effects	• Decide which processes, tools, and techniques would be available to deal with the effects of the cyberattack in each scenario.
Develop incident response plans	• What should your people do if an attack happens? Think about the people who own the information that is threatened. Also, consider each different part of the business — including corporate communications, media affairs, public relations, legal, marketing, law enforcement, and information technology. Document the actions and responsibilities for each, step by step, to get the business back to normal as quickly as possible. • Understand and periodically reassess vendor SLAs and contract terms to remain current with market, operational, and regulatory changes.
Decide what extra resources you need	• Define what you need to have ready — people, tools, or equipment — to deal with the effects of the cyberattack in each scenario.
Rehearse	• Finally, get everyone to practice the responses set out in the playbook for each scenario. This gives people experience in dealing with cyberattacks, and makes them less disruptive and damaging. Having a documented, practiced response to each kind of attack will make your organization much more cyber-resilient.

Investigate Notifications from Detection Engines

Security analysts receive thousands of alerts of potential incidents each day, often producing alert fatigue, which can result in missed signals and opportunities to prevent an attack from being successful. Incorporating contextual information around security alerts is, therefore, crucial to determining alert priority levels. Upon completion of this analysis, security incidents should be elevated based on established policy thresholds.

Leverage Technology to Automate Detection

The volume of data created when a firm is able to establish visibility into all network traffic, applications, and user behavior within an environment makes it difficult to identify the highest risk within a network. As a result, companies will need a series of capabilities to enable efficient and effective threat detection:

1. Implement log collection capabilities to consume a variety of feeds from the network, endpoint, and application layers.
2. Aggregate internal logs and external threat intelligence feeds to identify known signature-based attacks.
3. Identify and investigate anomalous, non-standard behavior in network, endpoint, and cloud environments for evidence of malicious activity, as not all attacks will be known or prevented.

The combination of these capabilities enables an organization to refine its focus for additional prevention activities.

Contain and Mitigate Incident

Security teams should take the corrective actions necessary to halt an ongoing attack, engaging external parties according to established plans if necessary to augment internal resources. Upon containment, organizations should take the necessary steps to mitigate the underlying vulnerability or point of compromise. To the extent practicable, organizations should endeavor to share this threat and mitigation information with external parties to leverage defensive network effects.

Incorporate Mitigations into Protection Mechanisms

In order to prevent similar attacks in the future, the protection mechanisms created to contain and mitigate incidents should be disseminated in an automated way to the relevant security technologies. The defensive technologies should also be reprogrammed automatically with these new protection mechanisms, similar to the response to a newly created protection mechanism against a previously unknown threat.

Conclusion: A Prevention Mindset

Perhaps because cybersecurity continues to evolve at a rapid pace, it may be tempting to revert to the same security measures that may have worked in the past. When aligning investments to match cybersecurity risk, there are two critical questions that leaders must ultimately ask themselves: how do we measure success, and what is the yardstick that allows us to validate the need for this change? In the dynamic arena of cybersecurity, continuing with the status quo approach because it may have worked in the past will do little to keep up with the asymmetrical economic dynamic underlying successful cyberattacks.

Business leaders should not assume that cyber adversaries will go away or that all attacks can be stopped. However, they should assume, and be very diligent in ensuring, that the cost of a successful attack can be dramatically increased to the point where the incidence of successful attacks will sharply decline. This is the outcome executives should strive for, as getting to this point would force attackers to expend considerable resources to design and develop unique attacks each time they seek to compromise an organization. Achieving this outcome will require a state-of-the-art approach to cybersecurity, which necessitates continual assessment, review, and revision based on changing business drivers, new technology adoption, and the evolving threat landscape.

Beginning with a prevention mindset is the first step in changing the economics of the cybersecurity challenge, which must be followed by action to change the status quo. Not every business leader needs to be a cybersecurity expert, but executives must be aware of the importance of our digital systems for customers, services, and missions. Companies have a new responsibility to change the way of thinking to make preventing cyberattacks a whole of community effort, approaching cybersecurity as a risk management issue and seeking to minimize those risks through sharing best practices, use cases, and cyber intelligence. Taking a longer view of the threat, the combination of next-generation technology and such joint efforts can reduce the number of successful cyberattacks and ensure the trust required for our digital age.

About Palo Alto Networks

As the next-generation security company, we are leading a new era in cybersecurity by safely enabling all applications and preventing advanced threats from achieving their objectives for tens of thousands of organizations around the world.

Find out more by visiting www.paloaltonetworks.com

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

pan-wp-aws-hybrid-design-guidelines-051216