How to Enable Cybersecurity Accountability for the Enterprise

SPONSORED BY ProcessUnity

NEXT ▶▶

Executive Summary

Budgetary pressures and regulations such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), the Health Insurance Portability and Accountability Act (HIPPA) and similar and similar statutes around the world have sharpened the focus on cybersecurity accountability in recent years.

Chief information security officers (CISOs) and other security leaders are increasingly being challenged to demonstrate that their organization — and associated third parties — have policies, processes and controls in place to protect enterprise data in a manner compliant with regulatory and industry standards. If something goes wrong, the security group needs to be able to quickly identify what happened and track the incident back to its root cause. In today's business climate, boards of directors (BoDs) now want to know how effective the enterprise security program is at mitigating cybersecurity risk. They are putting growing pressure on CISOs to implement capabilities for measuring programs' and controls' effectiveness, proactively making course corrections where needed before an incident occurs. BoDs are also demanding better articulation of the results from prior enterprise investments in cybersecurity before they will increase those investments.

At many organizations, CISOs and security leaders have incomplete information on the status of the controls and processes that stakeholders have implemented for identifying and managing cybersecurity risks. These information "blind spots" exist because most of the metrics and data required to demonstrate cybersecurity accountability exists in silos across the organization. CISOs often do not have the visibility or the cross-functional influence that would be required to gather information from all the asset owners across the enterprise and third-party ecosystems. Once the CISO has painstakingly collected and vetted the data, now they are faced with the equally daunting task of relating the data and presenting this complex technical information to the C-suite in a manner that effectively communicates the organization's exposure and response to cybersecurity risk.

Increasingly, there is a requirement for cybersecurity program management that enables greater visibility across the enterprise. Metrics on security operations and product security are essential, but that data is provided at a level of micro detail that is required for fixing the problem, not for communicating the risk, root cause, and business impact to C-level executives and board members. CISOs also need to be able to inventory and assess high-value assets and to understand how those assets are mapped to enterprise-specific threats, risks, policies and control standards, in order to provide business context to the cybersecurity risks. Security leaders need to have the ability to automate risk evaluations, perform control reviews, conduct application and system assessments, capture evidence of compliance on a scheduled basis and then synthesize all that data into an accurate "State of the Cybersecurity State" to the C-suite and BoD.

Why Cybersecurity Accountability Matters

Cybersecurity accountability refers to an organization's ability to demonstrate good cybersecurity practices. It is about security leaders being able to prove to the C-suite, BoDs, and regulators that the organization has:

- A plan and ability to defend against cyberattacks and protect the confidentiality, integrity and availability of business-critical data assets
- Controls and processes that are compliant with industry regulations and standard security frameworks
- The ability to trace security events back to a single unique source
- The ability to demonstrate overall effectiveness of the security program
- The ability to track improvements over time
- The ability to identify weaknesses and areas for improvement
- The ability to do all of this on a continuous and ongoing basis
- The means to prioritize the investment in risk-minimizing projects

Cybersecurity accountability emphasizes the notion of assigning risk ownership to specific individuals within the organization that have the authority to do something about those risks. Risk owners are responsible for identifying risks to assets under their control and for ensuring that processes for mitigating those risks are implemented correctly. They are responsible for communicating the status of assets under their control to security and risk leaders. The latest version of the ISO 27001[1] standard describes risk owners as being different from asset owners, who are the people responsible for running and maintaining critical business assets on a daily basis.

Data breach and compliance concerns are heightening the focus on cybersecurity accountability. Organizations that experience a major data breach can incur substantial financial cost, reputational and brand damage and customer churn. Companies that experience a breach can sometimes be subject to burdensome regulatory oversight for years.

Increasingly, BoDs and members of the C-suite are demanding more accountability for their past investments investments in cybersecurity. In approving security budgets and evaluating requests for increased spending, BoDs and other stakeholders expect security and risk leaders to explain how effective previous investments were in managing cybersecurity risk.

Organizations face threats to the confidentiality, integrity and availability of data on a variety of fronts and from a growing number of sources.

The fast-evolving nature of the threat landscape is another major factor. Organizations face threats to the confidentiality, integrity and availability of data on a variety of fronts and from a growing number of sources. Cyberattacks have become more targeted, persistent and financially damaging compared to a few years ago. Over the past two years ransomware and supply chain attacks have caused enormous business disruptions and financial losses to numerous organizations across multiple industries. Threat actors have become more organized, sophisticated and well-resourced. Many belong to large criminal groups with formal operational hierarchies and sophisticated models for monetizing attacks in a variety of ways. Organizations in critical infrastructure sectors are also under growing threat from state-sponsored threat groups looking to steal trade secrets and intellectual property.

Meanwhile, cloud adoption, enterprise mobility and other digital transformation initiatives have expanded the attack surface at many organizations in recent years. Data that once resided securely behind enterprise firewalls is now scattered across mobile devices, cloud systems and cloud services. The COVID-19 pandemic has exacerbated the issue by accelerating cloud and digital transformation initiatives and forcing a large-scale shift to a distributed remote work environment at numerous organizations. Attacks via vulnerable third-party systems and networks and the growing use of insecure open-source components in enterprise software have been growing concerns as well in recent years.

To manage risk effectively, CISOs and risk managers now require visibility into the state of cybersecurity across on-premise, cloud, mobile and third-party environments.

An Overload of Micro-Metrics

Forward-leaning security groups and those with mature cybersecurity practices have implemented numerous controls, policies and processes to manage these risks.

Tools are available to help organizations detect, respond, remedy and mitigate threats from the endpoint to the cloud. Data from SIEM platforms, network analysis tools, pen tests, threat modeling, security architecture reviews, threat intelligence feeds and more provide CISOs with a deep insight into the current status of their security operations and product security.

But often, there is a key gap in their ability to understand how effectively cybersecurity policies and controls are working to reduce cybersecurity risk at an

[1]https://www.iso.org/isoiec-27001-information-security.html

organizational level. Many security leaders struggle to identify where the biggest risks exist, what processes are in place to address those risks, whether those processes and controls are adequate or whether gaps exist that need to be addressed.

One major reason for this is a lack of visibility. Data that can help enable a complete picture of enterprise cybersecurity preparedness is typically distributed across business groups, asset owners, business systems and applications. CISOs often don't have the information and/or access to the information they require to inventory high-value assets across the enterprise or to assess the security status of these assets. The information and metrics that security and risk managers receive from asset owners and business groups tends to be "single threaded" and focused on a single domain of regulatory compliance or business risk. Security and risk professionals are left to the task of mapping the critical assets to specific threats, risks, policies and standards.

CISOs and risk managers managers typically have to access an abundance of micro-metrics pertaining to security operations and products. But they seldom have visibility into other equally important components of the enterprise cybersecurity program such as employee awareness and training programs; vendor risk-assessment processes; or compliance, audit or program management initiatives to manage cybersecurity risk. The lack of information around these key aspects of the security program often hampers CISO's ability to track improvements over time or to identify weaknesses and areas for strengthening.

Overly granular micro-metrics fail to provide the context that CISOs require to assess and to review enterprise-level threats and risk exposure or the policies and controls for managing them.

Cybersecurity Program Management

For true cybersecurity accountability, organizations need to bridge the gap that currently exists between executive leadership and

For true cybersecurity accountability, organizations need to bridge the gap that currently exists between executive leadership's perception and the complex domain of organizational data security.

where a lot of the key organizational security data resides.

CISOs can manage the cybersecurity program more effectively if they are able to collect and centralize organization-wide data on threats, risks, controls, policies, standards and regulations that are specific and relevant to the organization and its accountability and compliance requirements. They need to be able to verify that asset owners are following all mandated policies and processes for mapped threats, risks and controls. If gaps are identified, the CISO must be ready with specific recommendations and next steps for closing the gap or for maturing the program.

To ensure consistency and quality, CISOs require a standard way of collecting threat and control data from asset and risk owners. They need to be able to identify high-value assets and have access to data for conducting standards-based reviews of policy, controls, systems, applications, physical security and facilities. Access to third-party risk data is critical as well. Information on vendor vetting and onboarding and other data from vendor risks assessments, control assessments and ongoing monitoring efforts can all help CISOs gain a more holistic understanding of the enterprise's cybersecurity status.

When scoping the state of cybersecurity at the organization, the CISO should be able to baseline the security status across the enterprise. They need to then be able, on an ongoing basis, to measure deviations from that baseline via real-time visibility into the status of threats, risks, policies, security controls and events at an organizational level.

When communicating with the C-suite, security leaders need data that can help articulate threat history and trending, control coverage and effectiveness, incident reports and risk remediation status, due diligence requests and other topics at an enterprise-wide level. Data should be available that helps CISOs assess the "state of the state" for cybersecurity risk at the organization so that

they can better determine what kinds of projects to invest in or expand upon.

To address ad hoc demands for security updates from the BoD or C-suite, CISOs must have access to data that offers immediate insight into the status of threats, risks, controls and incidents across the enterprise. An automated process should be available to align cyber-risk activities that tie back to a single framework. There must also be an effective means of communicating security changes and incidents at the organizational level. Understanding policy accuracy, training program effectiveness, control alignment and key issues as they relate to company assets and third parties are essential to prioritizing investments and executive decision making.

Conclusion

To be able to demonstrate good security hygiene and compliance with regulatory and industry requirements, CISOs need enterprise-wide visibility into the state and effectiveness of their cybersecurity controls, policies and procedures.

Holistic cybersecurity program management is key to cybersecurity accountability because it enables this visibility. It enhances the CISO's ability to communicate effectively with the C-suite and BoDs. Most importantly, formal cybersecurity program management gives CISOs, risk managers and other security leaders a way to catalog and assess the risk exposure of an organization's most valuable business-critical assets. It provides visibility over the security preparedness of third parties and the risk they pose to the organization from a cybersecurity standpoint.

A formal program for cybersecurity management will help security managers determine if the controls and processes they have in place to protect enterprise data assets are adequate or need to be bolstered in order to manage cyber-risks effectively and in a manner compliant with regulations and internal standards. Now more than ever, understanding an organization's cybersecurity risk both internally and externally is critical to its ability to grow and adapt with the resiliency necessary to withstand unforeseen events.

About ProcessUnity

ProcessUnity's Cybersecurity Program Management enables organizations to reduce and manage cybersecurity threats and risks across applications, systems, facilities and third parties.

Combining a fully mapped control framework, automated workflows and best-practice assessments, ProcessUnity CPM delivers comprehensive, accurate and on-time information to meet the evolving demands of cybersecurity governance, risk and compliance.

ProcessUnity is used by the world's leading financial service firms and commercial enterprises. The company is headquartered outside Boston, Massachusetts. For more information, visit http://www.processunity.com.