ManageEngine
PAM360

Integrating risk management with cybersecurity

- Alan Rodger

www.manageengine.com/pam360

In the context of the accelerating change in business environment and their greater reliance on technology, CISOs need to prioritize security-related resources and investments, as well as prove that the value of spend on a security tool is fundamental to its credibility and scaling capability. CISOs must assimilate the right type and level of information, incorporate risk and compliance management, and implement tight security strategies that align with the organization's policies and business needs. The outcome should be that the protection of digital assets is managed dynamically at the appropriate strength and breadth to counter the risks that arise from both business operations and external sources, taking into account the value of information and brand assets and any related compliance obligations.

Dynamic business and cybersecurity contexts are driving the need for integration

Large-scale digitalization has deepened the dependence on IT

Very few technology trends have had anywhere near as profound an impact on business operating models as digitalization has. The subsequent impact on organizations has not been exclusively due to the complexity of technology adoption but rather to the changes in how organizations fundamentally operate across all business and IT functions. The IT capabilities underpinning business operations are ever closer and more critical to the success and fate of organizations of all types and sizes, and consequently, the need for enterprise governance to encompass the use and management of technology is indisputable.

In some of the most established industries, digitally-enabled change is causing large-scale consequences. Using banks as an example, the transfer

of funds has always been a key capability and foundation for them, but they have been hit hard by the increasing and disruptive availability and use of real-time payment systems and the encroachment of such consumer-led functionality into the corporate world. The direct impact is that banks can no longer support the needs of their corporate clients using systems and processes intended for a different era.

Core platforms are being replaced at a significant pace, with inevitable risks arising in key supporting processes such as fraud and risk functions that are also undergoing periods of relative instability. The key technologies that are the main sources of the opportunities available in digitalization are quite different in character to those of even 10 years ago. The massive impact of the cloud has now reached far and wide, but the cloud is still directly changing IT architecture and cost structures and enabling new business models. The explosion and ubiquity of intensive mobile usage has required the transformation of user experience and engagement. As the adoption of the internet of things (IoT) and artificial intelligence (AI) technologies continues to broaden, their impact is even more significant on business processes across different types of enterprises.

An important common factor across these technologies, however, is that a substantial proportion—in some cases the majority—of the resources and related supporting capabilities required are necessarily sourced on a continuing basis from outside the enterprise. This makes the control of related risks a greater challenge.

Any lack of insight can lead to technology being outpaced by dynamic business changes

Aside from the security issues arising directly from technology adoption, strategic business activities also give rise to cybersecurity challenges. Examples include:

- The formation of partnerships, which can involve arrangements such as sharing data and allowing access to corporate systems across organizational boundaries. Commitment to shared compliance responsibilities is fundamental for such arrangements, and this often creates security-related obligations that must be maintained in compliant status during the lifetime of the partnership. Even beyond that timescale, the obligation to prove that compliance can persist for a statutory period.

- Mergers and acquisitions, which commonly involve bringing together technologies, processes, data, and systems in new ways to serve different business imperatives than they originally served. Existing weaknesses must be assessed as part of due diligence in a compliance context, as well as the suitability of security arrangements for any ongoing changes in strategy.

Both of these examples illustrate situations that require organizations to understand any security issues in a business context. In the case of a merger or acquisition, understanding such issues is necessary to consider the effect in commercial terms. Within partnerships or other operational situations, business context is key to calculating the potential financial impact that any security issue could cause. Across the many technical and business situations in which understanding security issues is important, their diversity makes comparing them a significant challenge.

Security threats have become much more complex and ubiquitous

While risks arising from the extension of enterprises into modern technology environments can be assessed and managed to an extent, malicious actors now mount unprecedentedly complex and varied types of attacks more frequently than ever. These attacks can focus on weaknesses and vulnerabilities in any of the numerous technologies across now-broader

organizational IT estates (for example, cloud, IoT, and mobile devices), which have provided extensions to the attack surface available. The need to deal with a flow of innovative threat elements over time has driven the adoption of diverse protection technologies (i.e., security solutions).

Combatting attacks via vectors such as phishing, identity theft, hacking, and ransomware requires integration of people, processes, and these security solutions. Adapting resources to the changing volume, and the scale of some individual problems, is a major ongoing challenge for cybersecurity management, especially as both of these quantities are completely unpredictable. Increasing numbers of threats that may be relevant to an individual enterprise can overwhelm cybersecurity teams if they are uncertain of which threats constitute the most serious risk to their organization's assets and operations.

Cybersecurity and the growing compliance/ risk agenda

Compliance obligations are becoming more complex and require risk-focused capabilities

Regulations and legislation applicable in a number of industries require organizations to sustain risk-related practices. Many more organizations had to implement these practices when the EU General Data Protection Regulation (GDPR) came into play, as it applied to diverse organizations of all sizes in the EU and other regions globally. The GDPR requires a risk-based approach to data protection as a foundation for compliance, with specific stipulations such as:

- The recognition of high-risk activities with respect to maintaining appropriate levels of privacy.

- A level of data security appropriate to the risk that pertains to regulated data.

- An obligation to recognize if a breach of personal data is likely to result in a high risk to individuals' rights and freedoms and, if so, to notify the individuals affected.

However, risk is not clearly defined within the GDPR, so organizations must decide on (and document) their own means of appropriately assessing and managing risk in order to comply. Documenting the decisions made with respect to compliance and risk is of still greater importance to illustrate compliance with the GDPR's mandated organizational approach of establishing and maintaining "privacy by design and by default" and the need to undertake "data privacy impact assessments" within a process of risk-assessing any significant organizational change. Throughout these various considerations, risk is the primary driver for decision-making and should also be the arbiter of the level of security protection that is appropriate.

As such, organizations need mechanisms for integrating security with risk on an ongoing basis, as requirements and threat dynamics both reflect change. It should be understood that the GDPR is not the only legislative/regulatory driver in this area—many organizations operating in the US are also forced to consider this due to the California Consumer Privacy Act (CCPA). Also, globally, the National Institute of Standards and Technology (NIST) standards and the International Association of Privacy Professionals (IAPP) guidelines are strong sources of influence towards risk-oriented practices.

Compliance obligations are direct drivers of many security requirements

Many organizations' security-oriented compliance obligations historically arose from choosing to adhere to a framework or standard (or in some industries, a regulatory requirement to do so), such as ISO 27001 for information security. However, the inclusion of security stipulations within broader-scope regulations (i.e., the GDPR and other privacy legislation) has deepened the link between
security and compliance.

Like some risk mitigation measures, compliance management can be operated by sets of controls, which break down the overall scope of compliance obligations into actionable, measurable checks. In order to prevent unnecessary proliferation of controls, opportunities to use individual controls to fulfill multiple obligations should be implemented. Controls may be actioned by the activities of people, processes, or technology where compliance is a consideration. Examples of technologies operating security controls include:

- Authentication solutions, by enforcing the strength and security of access credentials. A particularly important example is the privileged access management (PAM) solutions category, as inadequate security around the most powerful credentials has been responsible for some of the largest-scale losses of personal data.

- Firewalls, by controlling network traffic as per the requirements of various standards and regulations (i.e. ISO 27001, NIST, and PCI DSS).

- Intrusion detection systems, by supporting analysis of events in to detect system-level attacks.

Compliance responsibility extends to vendor relationships, and security is no exception. Parties generally agree to adopt industry standards or frameworks relating to security, as there are suitable examples for common compliance obligations like ISO 27017 (security for cloud service providers), or the NIST Cybersecurity Framework. There are often wider benefits from adopting such standards, amongst which are the adoption of practices that help with future compliance requirements or deal more effectively with obligations from multiple sources. Skills availability is also segmented by industry standards, enabling standards-based compliance to be more sustainable.

Risk is an ideal "language" for ensuring broader understanding and communication of security issues

Malicious actors now mount unprecedented levels and varieties of attack, deliberately exploiting the complexity of organizational IT environments as a bigger target area. Dealing with threats can involve integrated understanding of attack vectors such as phishing, identity theft, hacking, and ransomware, as multiple modes of compromise are increasingly likely to be set in motion by the most sophisticated attacks. Organizations must be watchful over high-level threat intelligence to assess how the organization's protection can withstand current and emergent threats. With the scale of possible damage evident from the likes of WannaCry and NotPetya, senior management may have to be informed urgently about necessary mitigation measures or damage assessment if an attack is under way. Risk concepts and metrics are by far the most valuable means of communication and discussion in such situations, and an inability to meet this requirement can cost time, miss opportunities, and result in risk turning into loss.

Vulnerabilities are another continually-changing external threat that require organizations to regularly reassess their protection measures.

Discerning which vulnerabilities pose the greatest risk to the enterprise requires knowledge of which vulnerable technologies are present in organizational IT environments and what scale of risk could arise if the vulnerability were exploited in an attack. Assessment of that risk depends on what resources are based on the technologies in question, i.e,. the risk is greater if critical data or applications could be compromised. Technologies within an organization's digital supply chain are as relevant to these considerations of risk as those used or owned directly. Obvious examples include third-party cloud or software as a service (SaaS) providers' technology suites, but those providers and indeed all others will themselves have supplier relationships that involve potential security risks. Many failures and losses are known to result from such risks within third or nth parties' infrastructures, so governance capabilities should extend to understanding and mitigating potential risks, backed up by enforceable provisions defined in the supplier relationship.

How risk can inform security decisions

Over a prolonged period, the security solution market saw new products continually emerging to meet constantly changing threats and challenges. Partly as a result, many organizations' investments in security protection have been seen as a "black hole" into which experts advised funds must be committed in the hope of achieving the right protection, without any return on investment being promised up front or identified subsequently.

A risk-based approach to security investment can transform this picture. Individual risks can be quantified, and the cost of providing protection to counter them can be balanced against business value to assess whether a benefit for the organization results from a particular action. Taking into account all the relevant factors relating to a risk from across different areas of the organization enables the avoidance of siloed or partially valid decision-making.

Maximizing organizational benefit requires a risk-oriented approach to be consistently used to integrate security solutions. Where possible, this should extend to integrating with business applications, assessing whether user behavior or particular transactions represent risk, and adjusting the level of security applied, if that is required as a response.

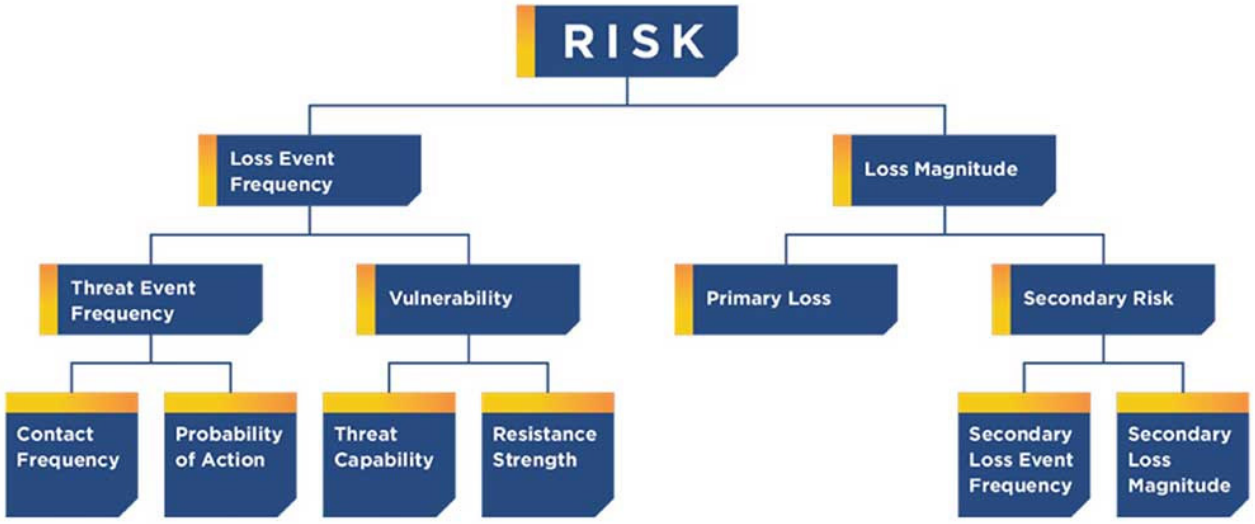
As well as enabling business-oriented decisions about security investment, risk-based analysis provides a common metric that allows disparate organizational functions to collaborate on the approach to threats or to weaknesses in protection. Investing in capabilities that provide risk metrics provides a foundation for increasing the reliability of decision-making and applying automation to this process when organizational maturity is at the appropriate levels. Improvements in AI technologies hold promise for more insightful automation to be available in future, with likely benefits being increased reliability and built-in advanced practices without cost-of-expertise issues.

Improving risk quantification is a key capability

Assessing cyber risk relating to actual organizational assets is complex and too involved and dynamic to be achieved manually in most organizational settings. Skills are also an issue, as not many organizations have the necessary resources in-house or to spend on adequate consulting to achieve this. In the past, there has been a clear functional gap between governance, risk, and compliance (GRC) operations, and security solutions. Using qualitative analysis of risk has always been limited by subjective content. Risk ratings are proprietary, and other categorizations of external factors lack integration to enterprise asset data to complete the perspective, and so cannot deliver an enterprise-specific risk evaluation. However, quantitative analysis incorporates insight into the potential impact (i.e., loss) that could result if a security issue hits the enterprise. Using this information, security leaders can present solution options that

combat a specific issue and compare the cost of each security option against the expected reduction in financial impact.

Solutions in the separate market segments would best serve enterprises if they worked with some standardized means of quantifying risk. Now, there is promise of exactly this approach from a well-established model (see the figure below) that is considered favorable by industry bodies. The management of the model—named Factor Analysis of Information Risk (FAIR)—is the responsibility of the FAIR Institute, which has leadership involvement from both tech companies and large enterprises. Importantly, The Open Group, which has long taken a leadership position towards establishing new tech-related standards where needed, is also involved with the institute.



Source: FAIR Institute

www.manageengine.com/pam360

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.manageengine.com/pam360

ManageEngine
PAM360