Ovum
TMT intelligence | informa

Business-Driven Security: An Essential Approach to Enterprise Protection and Compliance

Risk-enabled integration of security with business priorities is key to achieving the right protection

Publication Date: May 9, 2018

Author: Alan Rodger

Summary

In brief

IT security is increasingly critical to digitalized business operations and higher than ever before on board agendas, but it is often poorly understood and felt to be separated from organizational needs. Business leaders need to change this, and ensure that their security approach matures to be at least under the control of the business – ideally, driven by the business.

Risk acts as the critical link between business and security concerns, and is the ideal means for business to exert the control needed. Some of the many business contexts of risk illustrate its strength as the foundation of a common approach, such as its now-prominent position in regulatory contexts, its relation to potential business advantage, and the quantified benefits of security measures that counter specific threats and the risk they represent. It also enables business-level collaboration with IT experts that are pivotal to innovation and business momentum in the digital age, as well as providing a quantitative basis for the automation of security operations, which is essential to cater to performance-, capacity-, and complexity-related demands.

Integrating risk management and security solutions can provide the means to enable an understanding of the organization-specific context of risk, and to apply risk as the control mechanism across a range of key protection capabilities – i.e. business-driven security.

Ovum view

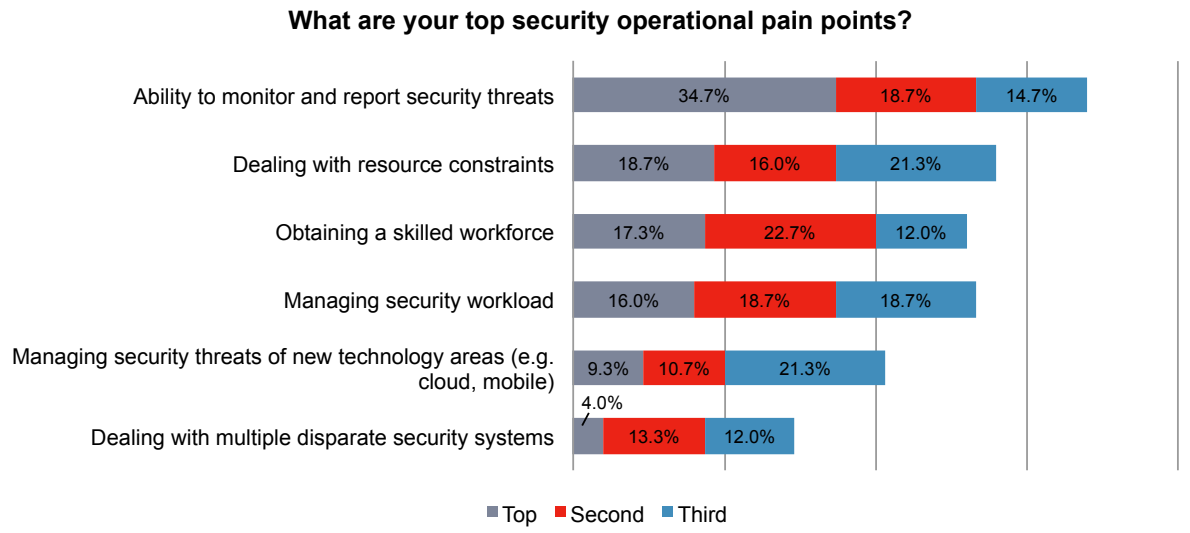
Ovum research shows that many enterprises are failing to maintain control of how their security investments address the threats they face (see Figure 1). According to our survey*, gaining visibility of security threats is one of their top concerns, followed by doubt about their capacity and capabilities to counter threats that continue to multiply. These problems are recognized by our survey respondents as being worsened by new technologies that are also sources of threats, and the complexity that has arisen in the multiple, disparate security systems that organizations struggle to manage.

Further detail (illustrated in Figure 2) shows that the great majority of our respondents unfortunately admit that the complexity of their own security systems has a negative impact on their protection, by

- causing additional risks that require further effort to manage, driving up costs
- reducing the effectiveness of security strategy, and damaging responsiveness to evolving threats
- causing strategic risk by reducing effectiveness in dealing with the challenge of security breaches (which is becoming a key capability due to more stringent compliance obligations and related penalties).

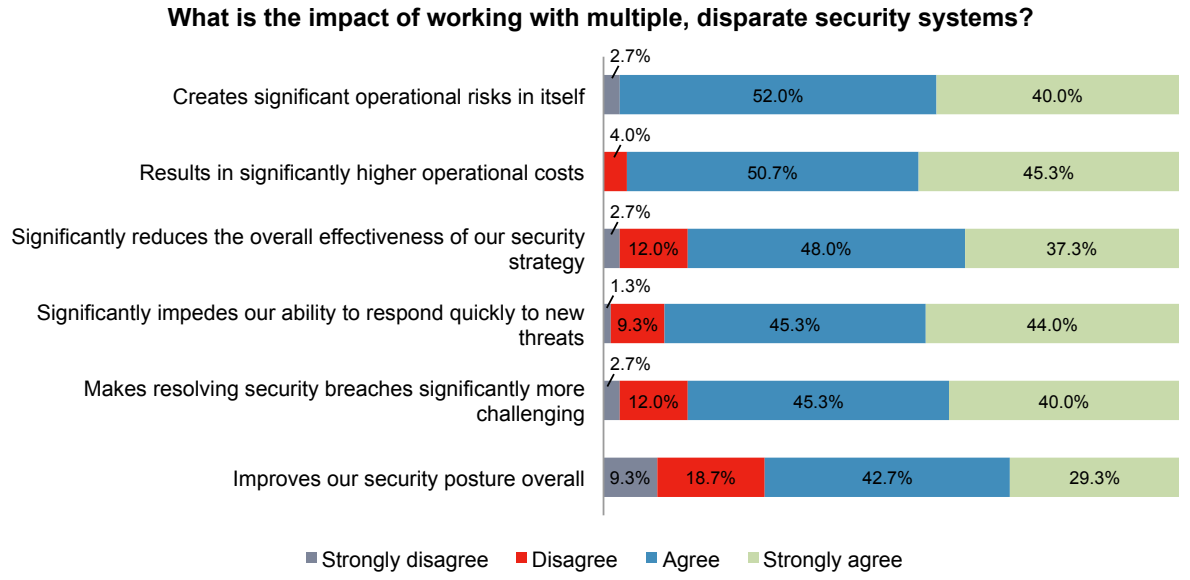
Organizations in such a position have no choice but to turn this situation around, or they could face potentially severe operational and financial damage from their inability to deal with increasing risks, compliance responsibilities, and cybersecurity threats. We firmly believe that strong governance, incorporating risk and compliance management, must drive security protection directly, ensuring that it meets the organization's business objectives – and that protection is managed with the appropriate strength and breadth to counter the risks that arise from business operations.

Figure 1: Security operational pain points



Source: Ovum*

Figure 2: The impact of security systems' complexity



Source: Ovum*

**Ovum spoke to tier-1, -2, and -3 financial services institutions (FSIs) in North America, EMEA, and Asia-Pacific. Tier-1, -2, and -3 FSIs here are institutions with assets of $100bn or more, $50bn–100bn, and less than $50bn, respectively. Of the FSIs surveyed, 25% have assets of more than $250bn and 50% have $10bn–50bn. Participating FSIs include retail banks, investment banks, and asset and wealth management firms. The individual respondents are decision-makers with job titles including chief information officer (CIO), chief information security officer (CISO), head of fraud, and head of risk and compliance.*

Key messages

- IT's pivotal role in business operations increases the consequences of digital risks to the enterprise. Additionally, the requirements for businesses to embrace digital transformation make it impossible to avoid these risks.
- Growing and diverse compliance obligations necessitate security's integration with governance.
- Business-driven security enables risk to inform security-related decisions and outcomes.
- Organizations should align their solutions and capabilities as a foundation for business-driven security.

IT's pivotal role in business increases the consequences of digital risks to the enterprise, and digital transformation makes it impossible to avoid these risks

Digitalization has deeply influenced organizations of all types

Very few technology trends have had anywhere near as profound an impact on business operating models as the digital mega-trend. 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 functions, from business to IT. The IT capabilities underpinning business operations are ever 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 waves, rather than ripples, in terms of consequences. Using banks as an example, the transfer of funds has always been a key capability and foundation for them, but they are being hit hard by the increasing and disruptive availability and use of real-time payments 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, and core platforms are being replaced at 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. The massive impact of cloud has now reached far and wide, but cloud is still directly causing change to 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 internet of things (IoT) and artificial intelligence (AI) technologies continues to broaden, their impact is also likely to be closer to business processes, and to have dynamic and variable consequences across different types of enterprise. An important

common factor across these technologies, though, 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.

Enterprises no longer have IT boundaries to form the scope of a protection landscape

The IT security challenge has evolved significantly in just a few short years. Long gone are the days when security was all about protecting the hardware and software assets located within the data center. Perimeter security has become just a small part of the focus needed, as cloud, mobile, IoT, and AI technologies all enable or promise benefits from complex capabilities delivered in large part via external computing and network resources. Within this broader, highly interconnected, and varied IT landscape the threats to digital assets abound, and strong protection is more important than ever – but it must be extended across a far broader and largely uncharted landscape. Given the cost challenges and impracticality of dealing individually with the myriad situations that may be encountered, a common basis for protection is needed, and **identity** has emerged as enabling organizations to manage access to resources while giving end users convenience and ease of use.

As the common "thread" across the use of IT resources and business applications, identity offers a strong basis for the best detection of security issues arising across the many different internal and third-party platforms and devices that provide opportunities for threat proponents. Advanced use of authentication allows the flexibility to deal with low-risk access situations with maximized ease of use, while adjusting dynamically to stronger validation of authentication criteria if business factors such as application-level risk or elevated threats in the IT environment require this approach.

As well as diversifying and growing, the use of resources and services from outside the enterprise is subject to increasingly dynamic change, and this is leading enterprises to support an escalating number of relationships with third-party organizations. Governance and compliance standards necessitate the application of diligence and a contractual basis for each of these, as well as an assessment of various types of risk relating to the relationship, and agreement between all parties on service levels and the support of incident management processes. Both of these aspects of the contractual relationship reflect business criticality, while the support of some types of incident management (e.g. reporting data breaches) has growing importance in the context of direct regulatory obligations.

Dealing with new risks is a consequence of digitalization

The recognition that new risks are an unavoidable element of enterprises' strategic advance toward greater digitalization is reflected in responses to Ovum's 2017/18 Global ICT Enterprise Insights survey. In several areas of investment supporting digital transformation, almost 80% of respondents had made initial or substantial progress toward establishing a proactive approach to cybersecurity and digital risk. These capabilities were markedly more advanced than others requiring investment and commitment, reflecting their foundational importance.

With services underpinning digital business being more IT-intensive than ever, risks relating to the way in which internal and external service elements are combined attain greater significance. For example:

- Reputation risk can extend along supply chains bidirectionally, leading to potential requirements to terminate existing partner relationships and quickly establish replacement ones to maintain service availability while avoiding reputation damage by association. Some social media campaign strategies have successfully targeted exactly this type of outcome.
- One-off certifications relating to aspects of partners' operations and management controls are no longer adequate proof of fit-for-purpose integrity and availability. Risk-based analysis of multiple information sources (including cybersecurity status) is an equivalent requirement for the digital era's more dynamic service environment.

Growing and diverse compliance obligations necessitate security's integration with governance

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. They will be joined by many more, as the EU General Data Protection Regulation (GDPR), which will apply to large numbers of diverse organizations in the EU and other global regions, requires a risk-based approach to data protection as a foundation for compliance. For example, specific stipulations require

- 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 the data
- an obligation to recognize if a personal data breach 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 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 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 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.

Enterprises must be able to integrate governance of broader, more diverse compliance requirements

The capability to deal effectively with risk and regulatory or legislative issues is key for competitiveness. As well as helping to avoid the sizable financial impact of noncompliance, it can better enable organizations to adapt to new obligations with reduced disruption, and even to enter new markets or adopt new business models more easily where these strategies involve extra compliance considerations.

The integration of governance, risk management, and compliance (GRC) practices across all areas of the organization is essential to achieving these and other benefits. As the number of compliance drivers increases, considerable efficiencies can be realized by dealing once with a requirement that is common across many obligations, thereby achieving multiple compliance benefits with one action. Requirements from relevant organizational functions such as audit, IT, and operational risk should all be represented in defining how compliance is to be attained, with a foundation of a data structure to deliver the insight necessary and avoid duplication of data and effort.

GRC solutions enable this approach by recording the segmentation of organizational obligations into control measures that enable compliance to be achieved. The status of the controls that map to a regulatory or legislative obligation enables overall compliance to be assessed. Where compliance requirements are common, individual control measures can be shared across multiple regulatory drivers. For example, a control measure that mandates a particular security stipulation might achieve compliance with several regulations, standards, or legal obligations.

Business-driven security enables risk to inform security-related decisions and outcomes

Risk should underpin business cases for security

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 not generating a return – as a "black hole" into which experts advised funds must be committed in the hope of achieving the right protection.

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 results. 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 increasing the level of security applied as a response. This can be achieved by "contextual security," which allows an application to call services that request stronger user authentication to better address increased risk.

The language and culture of risk enable cross-disciplinary collaboration on security decisions

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.

Organizations should align their solutions and capabilities as a foundation for business-driven security

GRC solutions address threats to organizational objectives

GRC solutions offer capabilities that enable governance to orient an organization toward its agreed objectives, and enable the following:

- Governance – integrating activities and information from different parts of the enterprise toward risk and compliance management, enabling analysis of these actors compared to the organization's objectives, and visibility/accountability at different levels of the structure.
- Risk management – recognizing and managing factors that could negatively affect the progress and outcomes of enterprise activities.
- Compliance – managing compliance with legislative and regulatory obligations, and with other undertakings such as standards.

IT is the source of particular types of risk, with GRC solutions enabling an understanding of how these translate into business risk, and to what areas of the business threats are directed. Making the right connections between IT risk, where the related business risk arises, and the related security protection that is in place (or needed) is becoming a key enterprise capability, which GRC solutions underpin.

Identity underpins all business relationships and the delivery and protection of services on all types of platform

Leading identity and access management (IAM) platforms have evolved continuously to enable security to be imposed appropriately for the diverse types of user populations that must be engaged in the digital age:

- Enterprise-native users undertaking different roles, using various applications and systems/resources.
- Users in B2B partners, authenticated via credentials held in partners' own trusted corporate identity directories.
- Cloud-based identity stores, often catering for very large-scale bases of consumers who self-register, with differing trust models of varying degrees of strength.
- In the near future, IoT devices, autonomously operating on an unprecedented scale of unstandardized diversity and volume, with limited scope to interact or supply sophisticated credentials.

Identity is the foundation for targeted, risk-aware security at the point of user interaction, on any type of access device or network. Additionally, the capability to indisputably link user identity with activity is critical to the analysis of behavior over any period of a business relationship, and hence to the identification of malicious, fraudulent, or unacceptably high-risk user activity. This can involve applying intelligence to associate different identities being used by individual bad actors or organized criminal groups, as well as the activity they undertake.

Cybersecurity applies intelligence to counter unforeseen threats that can develop rapidly

Protection against an increasing and ever-changing range of cybersecurity threats is now a high-profile focus of business leaders in most sectors. Solutions addressing this highly demanding requirement must apply intelligence in real time across a range of sources of information on emerging threats and on behaviors being experienced within and outside enterprise operations. The resulting analysis is needed to assess what adjustments to security controls on organizational activities and assets are necessary, taking into account risk-informed business priorities and compliance obligations.

On the defensive side of the cybersecurity arms race, automation is a critical component of survival. The widely acknowledged skills shortage in this domain, and the need for extremely rapid and ongoing reaction and the assimilation of massive amounts of data, are driving organizations inexorably toward leading-edge cybersecurity solutions that can integrate with other components to maintain sufficient strength and integrity of protection.

Appendix

Author

Alan Rodger, Senior Analyst, Infrastructure Solutions

alan.rodger@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum
TMT intelligence | informa

CONTACT US

www.ovum.com
analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo