JANUARY 2017

RISK

Protecting your critical digital assets: Not all systems and data are created equal

Top management must lead an enterprise-wide effort to find and protect critically important data, software, and systems as part of an integrated strategy to achieve digital resilience.

Piotr Kaminski, Chris Rezek, Wolf Richter, and Marc Sorel

The idea that some assets are extraordinary—of critical importance to a company—must be at the heart of an effective strategy to protect against cyber threats. Because in an increasingly digitized world, protecting everything equally is not an option. The digital business model is, however, entirely dependent on trust. If the customer interface is not secure, the risk can become existential. Systems breaches great and small have more than doubled in the past five years, and the attacks have grown in sophistication and complexity. Most large enterprises now recognize the severity of the issue but still treat it as a technical and control problem—even while acknowledging that their defenses will not likely keep pace with future attacks. These defenses, furthermore, are often designed to protect the perimeter of business operations and are applied disjointedly across different parts of the organization.

Our research and experience suggest that the next wave of innovation—customer applications, business processes, technology structures, and cybersecurity defenses—must be based on a business and technical approach that prioritizes the protection of critical information assets. We call the approach "digital resilience," a cross-functional strategy that identifies and assesses all vulnerabilities, defines goals on an enterprise-wide basis, and works out how best

to deliver them. A primary dimension of digital resilience is the identification and protection of the organization's digital crown jewels—the data, systems, and software applications that are essential to operations.

Burgeoning vulnerabilities, finite resources, fragmented priorities

In determining the priority assets to protect, organizations will confront external and internal challenges. Businesses, IT groups, and risk functions often have conflicting agendas and unclear working relationships. As a result, many organizations attempt to apply the same cyber-risk controls everywhere and equally, often wasting time and money but in some places not spending enough. Others apply sectional protections that leave some vital information assets vulnerable while focusing too closely on less critical ones. Cybersecurity budgets, meanwhile, compete for limited funds with technology investments intended to make the organization more competitive. The new tech investments, furthermore, can bring additional vulnerabilities.

The work to prioritize assets and risks, evaluate controls, and develop remediation plans can be a tedious, labor-intensive affair. Specialists must review thousands of risks and controls, and then make ratings based on individual judgment. Some organizations mistakenly approach this work as a compliance exercise rather than a crucial business process. Without prioritization, however, the organization will struggle to deploy resources effectively to reduce information-security risk. Dangers, meanwhile, will mount, and boards of directors will be unable to evaluate the security of the enterprise or whether the additional investment is paying off.

All data and systems are not created equal

In any given enterprise, some of the data, systems, and applications are more critical than others. Some are more exposed to risk, and some are more likely to be targeted. Critical assets and sensitivity levels also vary widely across sectors. For hospital systems, for example, the most sensitive asset is typically patient information; other data such as how the emergency room is functioning may even be publically available. Risks to priority data include breach, theft, and even ransom—recall that a Los Angeles hospital paid a $17,000 Bitcoin ransom to a hacker that had seized control of its systems. An aerospace-systems manufacturer, on the other hand, needs to protect intellectual property first and foremost, from systems designs to process methodologies. A financial-services company requires few controls for its marketing materials but is vulnerable to fraudulent transactions; its M&A database, furthermore, will need the best protection money can buy. Attackers can be individuals or organizations, such as criminal syndicates or governments with significant resources at their command. The attacks can be simple or sophisticated, the objectives varying from immediate financial reward to competitive or even geopolitical advantage.

Cybersecurity spending: When more is less

In the face of such diverse threats, companies often decide to spend more on cybersecurity, but they are not sure how they should go about it.

- A global financial-services company left cybersecurity investments mainly to the discretion of the chief information-security officer (CISO), within certain budget constraints. The security team was isolated from business leaders, and resulting controls were not focused on the information that the business felt was most important to protect.

- A healthcare provider made patient data its *only* priority. Other areas were neglected, such as confidential financial data relevant to big-dollar negotiations and protections against other risks such as alterations to internal data.

- A global mining concern focused on protecting its production and exploration data but failed to separate proprietary information from information that could be reconstructed from public sources. Thus, broadly available information was being protected using resources that could have been shifted to high-value data like internal communications on business negotiations.

These typical examples illustrate the need for a unified, enterprise-wide approach to cyber risk, involving the business and the risk, IT, and cybersecurity groups. The leaders of these groups must begin to work together, identifying and protecting the organization's critical digital assets as a priority. The process of addressing cyber risk will also have to become technologically enabled, through the implementation of workflow-management systems. Cybersecurity investment must be a key part of the business budget cycle and investment decisions must be more evidence-based and sensitive to changes.

The business-back, enterprise-wide approach

The key point is to start with the business problem, which requires a consideration of the whole enterprise, and then to prioritize critical risks. This work should be conducted by an enterprise-wide team composed of key individuals from the business, including those in product development, and the cybersecurity, IT, and risk functions. The team's main tasks are to determine which information assets are priorities for protection, how likely it is that they will be attacked, and how to protect them. In order to function, the team must successfully engage the leaders of several domains. They need to work together to discover what is most important—no mean challenge in itself. The best way to get started is to found the team on the agreement that cyber risks will be determined and prioritized on an enterprise-wide "business back" basis. In other words, the team will first of all serve the enterprise. Critical risks, including the impact of various threats and the likelihood of occurrence, will be evaluated according to the dangers they pose to the business as a whole.

Guiding principles

The following principles can help keep companies on track as they take the unified approach to prioritizing digital assets and risk:

- *Start with the business and its value chain.* The effort should be grounded in a view of the business and its value chain. The CISO's team, particularly when it is part of the IT organization, tends to begin with a list of applications, systems, and databases, and then develop a view of risks. There are two major flaws to this approach. First, it often misses key risks because these can emerge as systems work in combination. Second, the context is too technical to engage the business in decision making on changes and investments. By beginning with the business, the team encourages stakeholder engagement naturally, increasing the likelihood that systemic exposures will be identified.

- *The CISO must actively lead.* In addition to being a facilitator for the business's point of view, the CISO should bring his or her own view of the company's most important assets and risks. By actively engaging the business leaders and other stakeholders as full thought partners, the CISO will help establish the important relationships for fully informed decision making on investments and resource allocation. The role of the CISO may thus change dramatically, and the role description and skill profile should be adjusted accordingly.

- *Focus on how an information asset can be compromised.* If an information asset is exposed by a system being breached, the

vulnerability of this system should be considered, even if the system's primary purpose does not relate to this information asset.

- *Focus on prioritization, not perfect quantification.* The team needs only enough information to make decisions on priority assets. It does not need highly precise risk quantifications—these would be difficult to produce and would not make a difference in deciding between investment options.

- *Go deeper where needed.* The same level of analysis is not needed to quantify all risks. Only for particularly high-impact or complex risks should the team invest in deeper analyses. It should then decide on and acquire the information needed to make more informed investment decisions.

- *Take the attacker's view.* Risk reviews and vulnerability analyses must not focus solely on the value of the information to the company and the ascertainable gaps in its defenses. The profiles of potential attackers are also important: Who wants the organization's information? What skills do they possess? Thinking about likely attackers can help identify new gaps and direct investment to protect the information that is most valuable to the most capable foes.

A flexible systematic process with a designed platform

The object of the enterprise-wide approach is to identify and remediate gaps in existing control and security systems affecting critical assets. The solution, in our experience, will be an end-to-end process, likely requiring multiple development iterations, including a detailed account of hundreds of assets. A workflow system and asset database would be an ideal tool for supporting this complex process, allowing focus on prioritizing risks. A flexible, scalable, and secure online application can be easy to use while managing all the inventory and mapping data, the rigorous risk and control evaluations, sector-specific methodologies, and rationales for each risk level. The platform can also support detailed data to be used when needed as the team undertakes analysis of the priority assets and gaps and makes the recommendations that will shape remediation initiatives.

In developing this approach for clients, McKinsey experts defined the following five key steps:

1. *Identify and map digital assets, including data, systems, and applications, across the business value chain.* This can be accelerated by applying a generalized-sector value chain and a common taxonomy for information assets and then customizing these to the organization.

2. *Assess risks for each asset, using surveys and executive workshops.* By basing this analysis on the business importance of the asset, the organization will have identified its crown jewels.

3. *Identify potential attackers, the availability of assets to users, and current controls and security measures protecting the systems through which access can be gained to the assets,* using similar surveys and workshops as in step two.

4. *Locate where security is weakest around crown-jewel assets and identify the controls that should be in place* to protect them, by comparing the results of these assessments using dashboards.

5. *Create a set of initiatives to address the high-priority risks and control gaps.* Implementation will involve a multiyear plan, including

timelines for follow-up reviews. Once the initial assessment is complete, this plan becomes a living document, regularly refreshed to reflect new data, systems, applications, risks, and mapping, as well as progress to remediate known vulnerabilities (see sidebar, "An institution's progress").

The process promotes cyber-risk transparency, answering key stakeholder questions: What are our inherent information risks? Where is our organization vulnerable? How big (and where) is the residual exposure? What remediation actions should we prioritize? How do we know if what we did is working? Information-risk trade-offs can be defined based on a perspective on value at risk across the company. This helps the C-suite and board discuss information-security risk in terms of enterprise value, providing transparency on what risks they are willing to accept and why.

Results inform budget and investment decisions, helping to satisfy both regulatory and shareholder expectations. With investments targeted to best protect the most sensitive digital assets, costs are held down as the digital resilience of the organization is elevated. To build digital resilience

An institution's progress

One financial institution that used our approach was able to identify and remediate gaps in its control and security systems affecting critical assets. The change program began with a risk assessment that had highlighted several issues. Business and IT priorities on cybersecurity spending were found to be somewhat out of alignment, while communication on risks and risk appetite between risk management and businesses was less than optimal. The lack of agreement among stakeholder groups consequently stalled progress on a mitigation plan for cyber risk.

In response, the company established a unified group which together developed a work plan to protect critical data. The team inventoried all systems and applications in all business units, validating the results with key stakeholders to ensure completeness. They then identified critical data and performed a risk assessment with input from the stakeholders. The team was now able to identify the critical information assets based on potential risk impact. The level of control in each system was also evaluated, as the team mapped information assets to the systems and applications where they reside and isolated gaps between current and needed controls.

The critical data assets requiring additional protection were identified globally and by business unit. The systems and applications holding critical data that needed remediation could then be addressed. The team developed a series of detailed scenarios to reveal system vulnerabilities and help stakeholders understand what could happen in a breach. A comprehensive set of prioritized initiatives and a multiyear implementation plan was then created. The data resulting from this process are continually updated and provide guidance in budgeting decisions and board reviews on an ongoing basis.

into their operations, furthermore, the process can help organizations create periodic assessments to highlight trends and new gaps. Risk managers can then develop new initiatives prioritized to the enterprise's global needs.

■ ■ ■

Organizations in sectors with higher digital maturity will benefit the most from this approach, including financial services, manufacturing, and healthcare. They face the tough task of fully protecting their most important assets, while not stifling business innovation. To achieve this balance, the business, IT, risk, and other functions will have to work together toward the same, enterprise-wide end—to secure the crown jewels so that the senior leaders can confidently focus on innovation and growth. ■

Piotr Kaminski is a senior partner in McKinsey's New York office, **Chris Rezek** is a senior expert in the Boston office, **Wolf Richter** is a partner in the Berlin office, and **Marc Sorel** is a consultant in the Washington, DC, office.

The authors wish to thank Oliver Bevan and Rich Cracknell for their contributions to this article.