Digital Crown Jewels:
How to Protect Your Data Assets

Rotman

Protecting your organization's precious digital assets is no longer a choice, but a critical necessity.

"The potential cost of failing to act is far too great."

In the realm of cybersecurity, an important concept is that of 'digital crown jewels' (DCJs). These are your organization's most precious digital assets, and the analogy to priceless national ceremonial objects such as the Crown Jewels of the United Kingdom is apt: These assets must be protected at all costs from nefarious interference.

DCJs consist of in part an organization's data, and more specifically, the data that a firm possesses, processes and passes on that allows it to operate and deliver on its strategy. These data might include customer records, purchasing histories, employee records, finances and intellectual property information about proprietary products and services.

Such data are extremely valuable, and even more so when they contain personally identifiable information (PII) and personal health information (PHI). Data, however, are not the only valuables in need of protection. An organization's DCJs also include its data processing environment (DPE). This consists of both how data flows through the organization and the processes by which the firm and its agents access and manipulate these data. Failing to protect the DPE has and will continue to lead to notorious and costly digital breaches.

Consider the case of the 2020 **SolarWinds** breach. SolarWinds is a large U.S.-based software company specializing in information systems management tools, such as Orion, its IT monitoring system. More than 30,000 public (local, state and federal) agencies and private organizations like **Microsoft**, **Intel** and **Cisco** were using Orion to manage their information systems when computer hackers gained access to SolarWinds' system in September 2019. The hackers corrupted Orion's source code with malware that enabled them to access clients' data and information systems. The hackers also infected Orion's automated software updating process, such that when customers attempted the update (an automatic process much like software updates on a laptop computer), the malware would be automatically downloaded.

More than 18,000 unsuspecting SolarWinds customers installed the malicious update, causing the malware to propagate undetected. In turn, this allowed the hackers to install even more malware to spy on and steal from these victims. The insurance costs of this breach alone were estimated at US$90 million, not to mention the costs of reputational and brand damage and further unexpected cyber risk exposure for SolarWinds and its infected clients. In October 2022, SolarWinds agreed to pay shareholders $26 million to settle claims against the company and its directors. In addition, the **Securities and Exchange Commission** issued an enforcement notice that will have long-lasting effects.

Another cautionary example occurred in 2021 when remote management software provider **Kaseya's** update system was infected with malware. The virus was implanted by the

Russian criminal collective **REvil** into 60 of Kaseya's managed service providers (MSPs), resulting in over 1,500 unsuspecting customers downloading ransomware. MSPs are firms that provide and maintain information systems for end-user client organizations. REvil claimed to have infected over one million systems in this way and demanded a one-time payment of $70 million from Kaseya to provide a decryption key. Kaseya chose not to pay, instead deciding to rebuild its entire system at considerable cost in terms of time and money.

In both examples, these companies failed to properly protect their DCJs. Worse, as suppliers to many large corporations, they neglected to protect something that mattered just as much as their data: their software upgrading process. They consequently transferred supplier-induced cyber risk to their clients, resulting in a digital train wreck that was eminently preventable.

Elsewhere, **Colonial Pipeline**, a major supplier of fuel oil to the American Eastern Seaboard, was confronted in 2021 with a ransomware attack and a ransom demand of $4.4 million. As a vital part of American energy infrastructure (Colonial provides 45 per cent of the fuel for the East Coast), many assumed the company would be hardened and protected against such attacks. Yet, the attackers got into Colonial's network merely by using credentials from an employee who had left the company three years previously! To state the obvious, Colonial customers would have been severely affected had they run out of fuel in the dead of winter.

Like many organizations that have recently experienced cyber breaches, Colonial appears not to have considered user credentials (and the associated security processes required to keep them safe) as part of its DCJs. If it had, Colonial would have deleted them. That it did not is, unfortunately, not surprising based on existing cyber risk frameworks and models.

Too often, the DPE is not fully considered in DCJ assessments. Usually, the DPE is considered from a 'controls' perspective – and threat actors are continually searching for and unfortunately finding new ways to bypass controls. The result is a game of 'whack-a-mole,' where digital risk analysis is continually being assessed against the total number of controls on the DPE. Threat actors therefore look for alternate or unexpected paths to breach the perimeter of the DPEs that may not be protected as diligently as they should be, like unexpired access credentials. If effective cyber risk protection is to be achieved, the historic view of DCJs and their relationship to the must evolve.

According to **KnowBe4**, a cybercrime defense firm, the global cost of ransomware in 2021 was $20 billion. Left unchecked, these costs are expected to grow to an astounding $265 billion by 2031. The need to ensure that appropriate structures and processes are in place to reduce the potential for infection or cyber breach and the damage they cause is obvious. Most ransomware infections, for example, are the result of human error – such as employees inadvertently clicking on a link or downloading an attachment in a phishing email. Ongoing training, a cybersecurity-conscious culture, behavioural reinforcement and simple mechanisms like warnings in e-mails (i.e. 'Do not click on or open attachments from unknown senders') are critical.

Beyond such first steps, executives and managers need to broaden their understanding of DCJs by including the critical flows and processes that surround their data and DPEs in their risk analyses. They further need to consider the access paths that threat actors may attempt to exploit that have not historically been included in their cyber risk analyses – whether these paths have been technically compromised, socially engineered or sourced from an insider. Too often, in protecting the obvious, we neglect the more subtle, ancillary components of an enterprise that are at greatest risk.

Guidelines for Leaders

The list of actors who pose a threat to the integrity of a firm's data and DPE is long. It includes the freelancer working from home and ranges from there to petty criminals, organized crime, terrorists and state-sponsored hacking engaged in by nations who believe they are fighting a war on a non-traditional battlefield. Such actors pose various levels and types of risk, but they are all capable in their own way of inflicting severe harm on unsuspecting victims.

There is considerable evidence that the cybercrime industry is rapidly evolving, with actors specializing in various functions. For example, you will rarely be bargaining with the criminals that have ransomed you. These days, ransom negotiations are outsourced to specialists who work on commission and deal with multiple victims. Hackers are becoming as sophisticated as the organizations they prey on.

Cyber threats against an organization's data as well as its DPE should be considered as part of any organization's risk management system. These threats should be identified, assessed and managed according to such traditional risk management criteria as likelihood and impact. Threat actors, however, do not as a rule follow standard

enterprise risk protocols. It is thus important that a firm's leaders ensure the enterprise's risk management system reflects the complex and rapidly changing nature of the cyber risk landscape.

Cyber risk management therefore needs to reflect an understanding that cyber risk comes in not one but three primary forms: preventable, strategic and external. Let's take a closer look at each.

Preventable Cyber Risks

These risks reside within the organization itself and are thus entirely within an organization's control. They include employees who click on unknown links, or who fall prey to phishing scams or who download and use apps that pose intrinsic information privacy and other risks. Many Canadian governments, for example, have recently developed criteria to ban downloading of these types of apps onto government-owned hardware.

Such actions make sense because there are no redeeming virtues to being exposed to these types of cyber risks. Leaders, therefore, should take steps to drive such risks to zero, or at least to minimize them cost effectively. One way to do this involves education across the entire organization about proper 'IT hygiene' with respect to the DPE, from the most junior employee up to and including the Board of Directors. Other approaches include the dissemination and enforcement of rules. In short, leaders need to create, nurture and sustain an internal culture of control and compliance to minimize preventable threats to the organization's data and DPE.

Preventable cyber risks also include those posed by a firm's customers or clients. For example, customers reusing credentials can lead to a breach when those credentials are stolen and used to gain entry at multiple sites. This is what happened to **Canada Post** in 2019 when it was victimized in a 'cred stuffing' attack. To mitigate such risks, firms first must be aware of them. Customers, for example, could then be required to use multi-factor authentication (MFA) before being allowed to access the firm's website. MFA reduces cyber risk significantly, albeit at the cost of exposure to other risks, including increased friction at the customer interface and subsequent damage to firm revenues and profits.

Strategic Cyber Risks

This type of risk is taken to achieve the organization's most important, value-creating objectives. These objectives, typically described in a firm's strategic plan, might involve specific initiatives like market positioning and competitive analyses, cost and pricing information, new product and client development, expansion plans and even intellectual property such as patents, unique processes, innovations and inventions.

Equifax, for example, is in the credit rating and reporting business. To do what it does, Equifax needs to gather, manipulate and retain a massive amount of sensitive information. In 2017, Equifax was breached and over 150 million of its credit records were stolen. This was simply the result of a failure to patch the firm's software in a timely manner, leaving the company's entire database open to thieves. Equifax did not consider its software patching process to be a DCJ, trusting instead what turned out to be a flawed verification process. When executives asked if the system had been patched, they meant to ask if the software had been updated and the loophole closed. What IT management thought the executives were asking was whether the patch was queued and therefore in the process of being verified and authenticated before installation. The ensuing one-month gap between verification and installation led to theft of the sum total of Equifax's strategic value – a breach that has cost the company billions, and the CEO, CIO, CISO, CMO and general counsel their jobs.

Very few strategic objectives entail exposure to zero risk. The pursuit of different objectives to create value and obtain competitive advantage inevitably entails exposure to distinct types and levels of risk. Some strategic initiatives intrinsically involve exposure to more digital risk than others. Generally, the greater the IT content in a business project, the greater the exposure to cyber risk as a by-product of pursuing that business project. For example, transitioning from a bricks-and-mortar to a web-based retail strategy entails more and different exposure to cyber risk than would the opposite transition.

It makes sense to seek out strategic objectives and exposure to the risks that the pursuit of such objectives entails, assuming one believes one will be compensated or rewarded for doing so. But such risks should, if possible, still be reduced, transferred or insured against. Cyber risks, despite being taken in the pursuit of superior returns, can still imperil even well-established organizations. Appropriate steps therefore need to be taken to ensure that, if this happens, the damage will be less than fatal.

Strategic cyber risks have some desirable attributes, but it is often hard to distinguish such risks from others. The taking of cyber risks for strategic purposes places a premium on managers' ability to have a constructive debate and even engage in something akin to an adult conversation about

the nature and value of such risks and how they can best be addressed. Such abilities are not likely to flourish unless leaders establish a culture of constructive confrontation within the top management team and the boardroom that provides an organization's leadership with the opportunity to develop a realistic understanding of the cost, benefits and risks involved in any strategic IT initiative, and the measures needed to contain them.

External Cyber Risks

The fact that a risk originates externally does not mean it can't be identified or that steps can't be taken in advance to minimize the fallout that exposure to such risks entails. Sources of external cyber threats may include nation states such as China, Russia, Iran or North Korea. Other sources may not be as obvious, such as COVID-19, which induced organizations to either neglect cyber risk or accelerate their digital transformations without prioritizing security. The effective risk management of external threats to a firm's DCJs places a premium on a firm's leaders' ability to imagine, identify and prioritize such risks. Such threats also challenge a firm's ability to design effective responses as well as to stress test those responses before they are required.

For example, all firms need to formulate business continuity and disaster recovery (BC/DR) plans to help them respond effectively when they are breached. Imagine that your firm's BC/DR plans had been obtained by hackers before a successful breach. This may sound far-fetched, but once these plans exist in electronic form, and are stored on your company's servers, they become a target. Less difficult to imagine is the havoc a cybercriminal could wreak with advance complete knowledge of your firm's response plans.

The purpose of risk management is not to induce paranoia and panic attacks but rather to allow leaders to manage the firm's digital risk exposure to keep it within the organization's risk appetite. So, important but frequently unasked questions for leaders are: How much cyber risk are we prepared to seek out or retain in quest of our business objectives? How much risk appetite do we have for exposure to digital risk by failing to practise proper cyber hygiene within our DPE?

Failure to ask these kinds of questions – or asking them without formulating an actionable and measurable response – can induce either excessive conservatism in managers paralyzed by the thought of something going wrong, or complacency and a propensity for the taking of severe and unjustifiable digital risks. Neither of these reactions is usually performance or career-enhancing. To encourage appropriate levels of cyber risk taking, managers need to understand whether the avoidance, mitigation, transference or embracing of all types of cyber risk is a core objective.

Other ways leaders can ensure their organizations' cybersecurity policies, practices and procedures are gold standard with respect to the myriad threats to their DCJs involve the setting of specific and ambitious goals in this regard. Not only should such goals be set (i.e. 'The organization will have attained state-of-the art cyber maturity within 12 months'), but also adequate funding for the attainment of such goals should be provided. Further, managers should be rewarded contingent on goal attainment. To ensure such goals are accepted by those expected to implement them, leaders should officially announce their and their organization's commitment to such goals. Abundant evidence supports the view that specific and ambitious goals that are also widely accepted result in both strong motivation and high performance.

Digital Crown Jewels:
How to Protect Your Data Assets

Rotman

In closing

The widely understood notion of 'loss aversion' teaches us that losses are felt more intensely than comparable gains. As a result, getting managers to consider the consequences of failing to act on any initiative will be much more motivating than having them focus on the potential benefits if they do act. To get started on protecting your digital crown jewels, begin by asking: 'What are the possible consequences of failing to protect our most precious digital assets in the best conceivable way?' As indicated herein, the potential cost of failing to act is far too great.

This article originally appeared in the Fall 2023 issue of Rotman Management magazine.

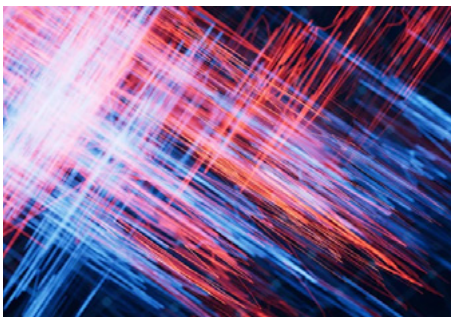
Michael Parent is a Professor of Management Information Systems at Simon Fraser University's Beedie School of Business and Academic Director of the Rotman and Institute of Corporate Directors' Directors Education Program in Vancouver and Montreal.

Greg Murray serves as Cyber Security and Technology Director-in-Residence for Rotman's ICD Directors Education Program. He is also Co-Chair of the Canadian Security Telecommunications Advisory Committee and a board member of the Canadian Institute for Cybersecurity.

Glen Whyte is a Professor of Organizational Behaviour at the Rotman School of Management and Academic Director of the Rotman and Institute of Corporate Directors' Directors Education Program in Toronto.

If you liked this article, you might enjoy these:

Are the right ESG risks on your radar?



Social progress isn't linear, but people believe it is

Why it's time to move fast and fix things

For more groundbreaking ideas like these, please visit:
Rotman Management Magazine or the Rotman Insights Hub