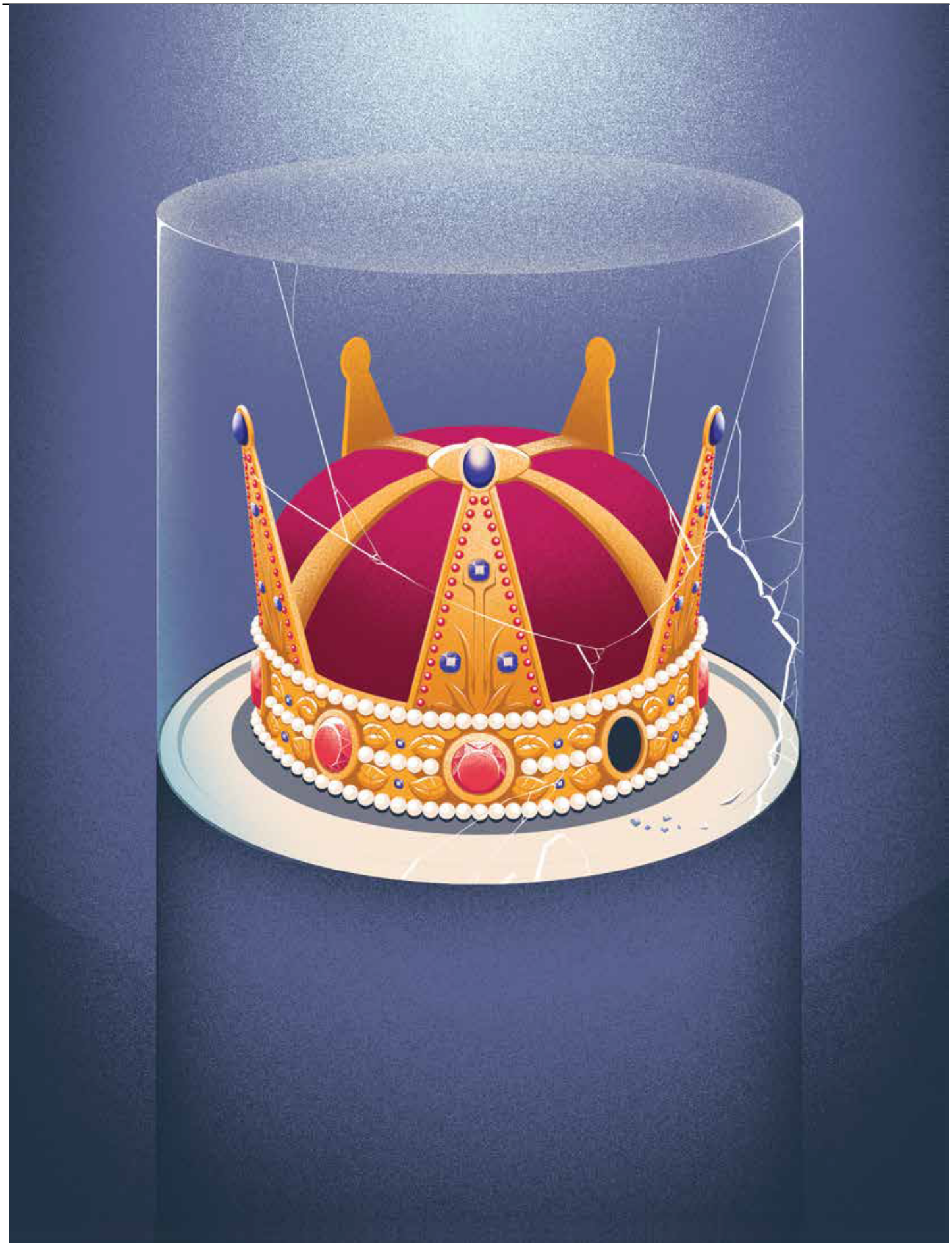
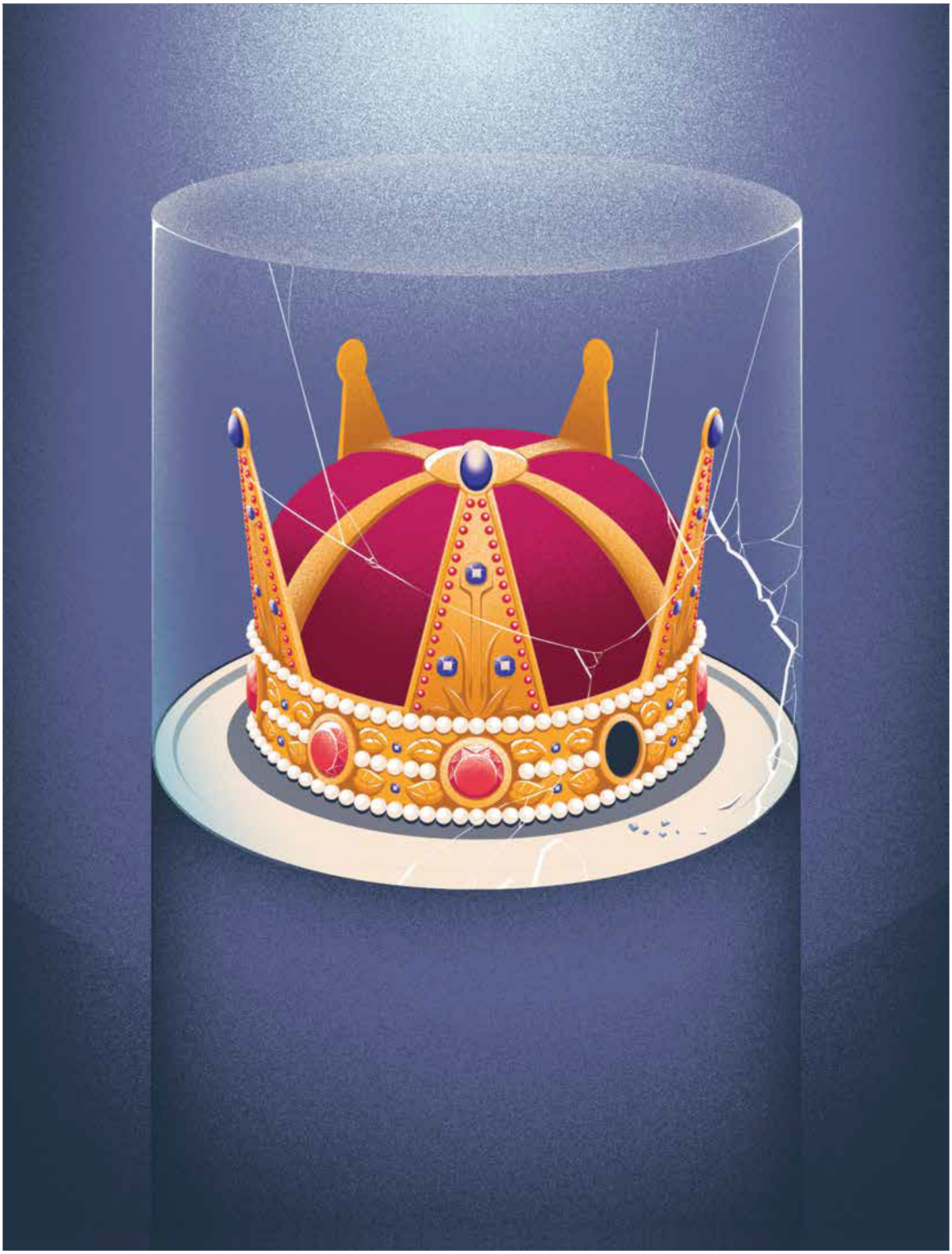
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Cover Your Assets

Intellectual Property

Technology, Privacy, and eCommerce





CHEAT SHEET

- ***Define and conquer.*** Knowledge assets are best defined as the confidential information that is critical to the company's core business. The loss of such assets can affect the company not only financially but also through its brand and reputation.
- ***Knowing the risk.*** Given the level of risk to an organization that does not have the necessary expertise regarding knowledge assets, implementing and ensuring appropriate protection will continue to be an uphill battle. It is estimated that there are over a million unfulfilled cybersecurity and information security positions globally.
- ***Inform to insure.*** Despite the consequences, most board directors are not informed of the steps taken to secure knowledge assets. In-house counsel should take a leadership role in educating the board on the importance of data protection and creating a classifying system that segments information based on value or priority to the organization.
- ***The crown jewel.*** To protect a company's most sensitive data, in-house counsel should initiate a formal knowledge asset program to make security a top priority. It's imperative to ensure transparency with senior management so they understand the risk.

Personal data. When those two words are read, we automatically start thinking about privacy laws and requirements. But why don't we think about knowledge assets? Some people might wonder what a knowledge asset is and why it matters. Many already know what knowledge assets are, but the phrase does not bring to mind data protection measures or specific controls. Yet knowledge assets may be a company's greatest resource and, if lost, could cause utter destruction. Knowledge assets are best explained if one thinks of them as …

> *… the knowledge drivers of an organization's success. Knowledge assets can be unstructured, as tacit knowledge (e.g., key personnel with deep expertise). Or they can be structured, as explicit knowledge, and codified (e.g., patents, copyrights, and intellectual proprietary rights in codified form). What is interesting about knowledge assets is that the more you provide structure, meaning the more you codify knowledge, the easier it is to share both internally and externally. Structured knowledge can be shared in milliseconds via the internet, whereas deep expertise or experience requires more time to share with other people.*

Successfully managing knowledge assets leads to increased profits, especially due to advancements in technology and the changing role of intellectual property. In addition, knowledge assets are now created — and exploited — anywhere a company operates.

This article explores the realm of knowledge assets to understand the threats to protection and how to minimize those risks.

Understanding knowledge assets

When we think of knowledge assets, we often view them from the perspective of assets on a balance sheet. With a quick glance, identified items include fixed assets, current assets (anything with a

lifespan of less than one year that can easily be converted into cash or a cash equivalent), non-current tangible assets (a lifespan of more than one year: machinery, buildings, land), and intangible assets such as goodwill, patents, or copyrights. Even though intangible assets are not physical in nature, they are often the resources that can make or break a company — the value of a brand name, for instance, should not be underestimated.

> "Some day, on the corporate balance sheet, there will be an entry which reads, 'Information,' for in most cases, the information is more valuable than the hardware which processes it."
>
> Rear Admiral Grace Murray Hopper

Knowledge assets are confidential information. They comprise the information critical to a company's core business, other than the personal information that might trigger notice requirements under law. These include trade secrets along with other corporate confidential information such as profiles of high-value customers, product design, development and pricing, pre-release financial reports, strategic plans, confidential information about existing relationships or contemplated transactions, source code, or research and development secrets. These knowledge assets may be wholly within a company or reside with its partners or vendors.

> Knowledge assets are confidential information. They comprise the information critical to a company's core business, other than the personal information that might trigger notice requirements under law.

The loss of knowledge assets, often a company's most critical and sensitive, can affect a company not only financially but also tarnish its brand and reputation. A July 2016 report entitled The Cybersecurity Risk to Knowledge Assets, by the Kilpatrick Townsend law firm in collaboration with the Ponemon Institute, revealed that the average cost to remediate an attack involving knowledge assets is nearly US$5.5 million. The overall cost to organizations from the theft or loss of intellectual property and other knowledge assets ranged from US$100 million to US$150 million.

Understanding the threat to knowledge assets

The risk to knowledge assets is increasing, but protection is still difficult to achieve. Recently, a computer engineer was accused of stealing proprietary algorithms for trading models from his employer. The company protected the source code of its models and platforms with encryption keys and limited employee access and restrictions on the use of file-sharing websites and storage devices. The computer engineer took various steps to steal the source code, including installing a code that could scout out encryption keys in order to access portions of the source code and implementing another code that sent data from the firm's system to a third party software development site. It was discovered only when a part of the system was accessed where the engineer did not have permission, thus triggering improper-access alerts. If the security team did not flag the event, would it have been discovered? How long would it have taken? In another case, an employee was charged with stealing valuable, proprietary software from his former employer, an American company, that he intended to share with an agency within the Chinese government. These are just two of many examples of internal threats to knowledge assets.

Both insiders and third parties threaten the security of knowledge assets. The most significant threat is employee negligence. From the July 2016 survey, 59 percent of respondents say their

organizations restrict employee access to confidential information on a need-to-know basis. Need-to-know focuses on minimal access, permission, and the ability to control access information. The survey found that access control processes are often not reviewed, improperly deployed, and simply ineffective. Various scenarios are implicated here: Access permissions are not changed when an employee changes roles or duties, or access permissions are not reviewed and terminated when employees separate from the company.

This is also true for third parties who have access to systems. If contractors are engaged to work on projects and are subsequently reassigned, their access rights should be revoked. Once the engagement is completed, all rights should be terminated. Depending on the size of the organization and its global presence, this can be a daunting task. Ongoing audits should take place to determine who is accessing the systems, flag the exceptions, and validate corrective action.

Nation-state attacks are also a serious threat. The primary motivations of attackers who steal a company's knowledge assets are economic espionage, hacktivism, cyberwarfare, and sabotage. In his 2015 State of the Union address, former US President Barack Obama stated, "No foreign nation, no hacker should be able to shut down our networks, steal our trade secrets.… If we don't act, we'll leave our nation and our economy vulnerable." Economic espionage not only harms companies that have years of work stolen but also crushes the spirit of innovation and fair play in the global economy.

Do you Prezi?

Prezi is an online presentation software used by over 60 million users globally.

This is a common example of how knowledge assets are leaked out. When signing up for a "basic" Prezi account, your prezis will be publicly viewable, searchable, and reusable. There are currently 190 million public prezis around the world. How many of your employees use "basic" Prezi to prepare client presentations because of the enriched features and its convenience? Consider the content of those presentations; strategy, competitive pricing, market differentiators, and current client relationships. Read the terms of service, determine your level of risk, and educate your employees.

TERMS OF SERVICE

6.2 Licenses you grant to Prezi for use of Public User Content and Private User Content

With respect to Public User Content, you hereby do and shall grant to Prezi (and its successors, assigns, and third party service providers) a worldwide, non-exclusive, revocable, royalty-free, fully paid, sublicensable, and transferable license to use, host, store, reproduce, modify, create derivative works, communicate, publish, publicly perform, publicly display, distribute and transmit the content (1) for the purpose of providing you, and those with whom you have shared your presentations (including the public), with the Service; and (2) in connection with promotion and marketing of Prezi products and services, including without limitation allowing third parties to search or index the content, in connection with email promotions, product demonstrations, and the like. This license ends when you delete your Public User Content or your account is closed (either by you or by us), except (i) to the extent that your Public User Content has been shared with others and they have not deleted it and (ii) that we retain a license to maintain a back-up copy of your Public User Content indefinitely.

IT security professionals believe current approaches to protecting knowledge assets are ineffective. Less than one-third of the companies surveyed rated their ability to mitigate the loss or theft of knowledge assets by insiders and external attackers as highly effective. They attribute this to ineffective or improper access control and lack of employee awareness about information confidentiality. Those who said their current approaches are ineffective cite reasons pertaining to a lack of in-house expertise, clear leadership, and collaboration with other functions. The most difficult knowledge assets to secure are not appropriately safeguarded. Private communications such as emails, texts, social media, and product/market information are the most difficult to secure. Most companies do not secure these assets appropriately.

Given the level of risk exposure to an organization that does not have the expertise to protect its knowledge assets, implementing and ensuring appropriate protection will continue to be an uphill battle. Addressing these issues will not be easy for companies — one cannot merely go hire an expert; it is estimated that there are over a million unfilled cybersecurity and information security positions globally. Thus, companies are forced to take alternate measures to reduce the burden, such as using cloud providers, outsourcing security positions, and cross-training talented IT personnel. And yet, the threat remains.

What is a trade secret? The European Union compared to the United States

In Europe, Article 2 of the Trade Secrets Directive defines a trade secret as information that meets all of the following requirements:

- Is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- Has commercial value because it is secret;
- Has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret; and,
- This definition tracks the definition for “undisclosed information” provided in article 39(2) of the World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), which requires all signatories to afford some level of protection for confidential information.

The US Defend Trade Secrets Act defines trade secrets as “all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:

- The owner thereof has taken reasonable measures to keep such information secret; and,
- The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by another person who can obtain economic value from the disclosure or use of the information.”

Incidents involving knowledge assets

Being tried in the court of public opinion is not something that most corporate executives want to experience. They worry about data breaches that trigger breach notifications and regulatory oversight, even though the loss of knowledge assets could destroy a company. Careless and malicious insiders are the most likely cause for the loss of knowledge assets. Over 50 percent who replied to the survey indicated that senior management's concern focuses on data breaches that involve financial account information; because of these personal data elements, Social Security numbers trigger breach notification laws. Depending on state laws, notifications to the state attorney general, to law enforcement, and to the media may be mandatory. The same level of scrutiny does not appear to be associated with the loss of knowledge assets. Redress for theft or attempted theft of knowledge assets often falls within the Computer Fraud and Abuse Act (18 U.S. Code § 1030) or the new Defend Trade Secrets Act of 2016 (largely a reflection of state laws addressing the same topic). Europe has a directive issued in 2016 by the European Parliament and the European Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use, and disclosure.

Unauthorized access or disclosure (breaches) involving knowledge assets have multimillion-dollar consequences. Companies have seen upper limits reach as much as US$270 million, and the average cost to remediate attacks against knowledge assets in the past 12 months was US$5.4 million. This cost includes reputation loss and brand damage, disruption of operations, remediation and technical support activities, lost productivity due to system downtown time or performance issues, and the damage or theft of IT assets and infrastructure. Recent examples include hackers attacking Samsung in an attempt to steal the technology behind the Samsung Pay service; a complaint by US Steel Corp. to the International Trade Commission alleging that the Chinese steel industry (in collaboration with the Chinese government) stole the company's trade secrets; and an accusation that Chinese hackers perpetrated attacks on US technology and drug companies to acquire designs and research for unreleased products.

However, most of the cases under the Defend Trade Secrets Act are relatively mundane, referring to customer lists, otherwise known as "soft" trade secrets. These cases brought under the Defend Trade Secrets Act are instructional as to what makes a valid case for a soft trade secret, especially to grant an injunction barring the defendant from using the information. Let's look at some key points of the *First Western Capital Mgmt. Co. v. Malamed*, No. 16-cv-1961-WJM-MJW, 2016 WL 8358549 (D. Colo. Sept. 30, 2016) case, where the ex-employee allegedly took 130 pages of customer names (roughly 5,000 names) along with 22 pages of spreadsheets with market values of their holding and management fees.

- **Credibility:** Defendants will likely deny the factual elements, saying that the customer lists they took contain no confidential or sensitive information or that they do not know how to work common tools of technology, such as reading information from a disk. Witnesses (defendants) must be credible.
- **Intent:** Defendants must have an intent to use the trade secrets in a manner that may harm the company.
- **Risk of harm:** The defendant must have enough information that can be used to harm the company, such as price lists, order history, or strategic market plans.

Critical to the cases under the Defend Trade Secrets Act are whether customer lists even qualify as trade secrets (they do) and if so, must they be in digital or paper form (they do not). Customer lists qualify as trade secrets because they are valuable and, combined with purchasing history, fees

charged, and other such insider information, could be especially valuable to a competitor. Even remembering that such information may qualify as a trade secret is the first step. But it's only the first step in restricting a former employee from using the information against the company — proving that a single avenue to protection (security controls) may be insufficient to prevent harm. Companies must take the threat seriously and approach it from multiple perspectives.

Despite the cost of recover and remediation efforts, most boards of directors are not informed of the steps taken to secure knowledge assets. More alarmingly, less than one-quarter of boards are made aware of breaches involving the loss or theft of knowledge assets. A board's responsibility to understand and address risk on the cybersecurity front is a well-known and often bemoaned aspect of corporate governance. However, little research and few resources exist to address why this risk is not presented to the boards. Even less research exists as to why the protections that address risk to confidential personal data are not extended to knowledge assets. Companies need to have a process in place to understand what high-value information they must secure. Most companies have no data classification system that segments information assets based on value or priority to the organization.

Data classification and inventory

One needs to understand the criticality of the data in order to assess the risks to the data.[1]

Having a data classification scheme within an organization provides guidance to employees on what steps they need to take to protect the data. Data classification identifies its value to the organization and is critical to protecting confidentiality and integrity.[2]

Data classification schemes range from the least sensitive data to data that is considered highly restricted or strictly confidential. Between these two extremes would fall regulated data, confidential data, and data that falls within company only, etc. Companies should develop an information classification standard that considers legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification of the data.[3]

The more sensitive the data, the higher the degree of controls required to protect it. The need-to-know principle imposes the requirement to grant users access only to data or resources they need to perform an assigned task.[4]

Companies often classify personal data without classifying knowledge assets. Yet knowledge assets, a low percentage of the company information (less than two percent), comprise over 70 percent of the value. A proper data classification scheme would account for these crown jewels and even better — inventory them. These two elements form the foundation of a proper data protection program, feed into privacy impact assessments, and help establish good data hygiene among employees.

1 Dennedy, M; Fox, J; and Finneran, T. The Privacy Engineer's Manifesto. Getting From Policy to Code to QA Value. Page 251.

2 Stewart, J, Chapple, M, and Gibson, D (2015). CISSP(ISC)² Certified Information Systems Security Professional 7th Edition Indianapolis, IN: John Wiley & Sons, Inc, page 160.

3 Dennedy, M; Fox, J; and Finneran, T. (2014). The Privacy Engineer's Manifesto. Getting From Policy to Code to QA Value.Page 251.

4 Stewart, J; Chapple, M; and Gibson, D (2015). CISSP(ISC)² Certified Information Systems Security Professional 7th Ed. Indianapolis, IN: John Wiley & Sons, Inc., page 662.

How to protect knowledge assets

Given the disastrous consequences of losing knowledge assets in conjunction with the shortage of cybersecurity professionals who can implement and manage adequate controls, companies need to know some fundamental steps they can take to protect these crown jewels. Below are the top 10 actions that companies should take to protect knowledge assets.

1. Initiate a formal knowledge asset protection program. Make the protection of knowledge assets a priority and be transparent with senior management so they understand the risk caused by insecure knowledge assets. This includes educating the company's board.
2. Address employee negligence. The careless insider is the primary cause of a data breach involving knowledge assets, despite policies and training programs in place. It is not unheard of that a careless engineer may upload a drawing of a prototype to a free software vendor to get a 3D rendering or a marketing employee to use a free survey vendor to get feedback from beta testers. They intend no harm; they are simply careless and uninformed of the consequences to the company.
3. Require a formal incident response plan and audit protocol. Companies typically have an incident response plan, but it is often informal and ad hoc. Only one-quarter of respondents to the 2016 survey say their companies conduct formal assessments or audits to determine the cyber and data breach risks posed by insecure knowledge assets.
4. Align the knowledge asset protection program with the IT security strategy. The protection of knowledge assets should be an integral part of a company's IT security strategy.
5. Exercise centralized control over the protection of knowledge assets. The individuals most likely to determine the approach to securing knowledge assets are the chief information officer and the chief compliance officer. However, responsibility for protecting knowledge assets is dispersed throughout the organization.
6. Manage access to knowledge assets. The most likely root cause of a data breach involving knowledge assets is the careless employee, but half the survey respondents say both privileged and ordinary users have access to the company's knowledge assets.
7. Prevent access to knowledge assets from remote locations and restrict the use of personally owned mobile devices to reduce the risk.
8. Require strict safeguards when sharing knowledge assets with third parties, from contractual obligations to privacy and security controls. Often, companies will implement these safeguard requirements when personal data is involved, such as patient data or employee data, but neglect to do so when knowledge assets are in play.
9. Implement appropriate vendor management, especially with cloud vendors. Companies are storing knowledge assets in the cloud without careful vetting of the provider. Sixty-three percent of respondents say their company stores knowledge assets in the cloud. The most common steps taken to secure knowledge assets in the cloud are identity and access governance (56 percent of respondents), contracts with purported indemnification by the cloud provider (49 percent of respondents), and encryption of data in motion (45 percent of respondents). Only 33 percent of respondents say their companies carefully vet the cloud provider. Similarly, only 30 percent of respondents say they require proof that the cloud provider meets generally accepted security requirements, and only 23 percent of respondents

say their organizations require proof that the cloud provider adheres to compliance mandates.
10. Expand security measures to cover knowledge assets, such as encryption for data in motion and at rest along with identity management and authentication.

The study by Kilpatrick Townsend and the Ponemon Institute shows, while many companies have tools to better protect knowledge assets, they also lack the understanding of what they need to protect and why. Having identified the threats to the security of knowledge assets, the consequences resulting from a breach of knowledge assets, and the key factors in protecting knowledge assets, you are now in a better position to safeguard your company.

The authors would like to sincerely thank Jon Neiditz of Kilpatrick Thompson & Stockton, LLP, and Larry Ponemon of the Ponemon Institute for their expertise and collaboration and especially their report on this topic.

Further Reading

Stewart, J; Chapple, M; and Gibson, D (2015). CISSP(ISC)² Certified Information Systems Security Professional 7th Ed. Indianapolis, IN: John Wiley & Sons, Inc.

Morgan, Steve. “1 million cybersecurity job openings in 2017.” Cybersecurity Business Report. January 8. Dennedy, M; Fox, J; and Finneran, T (2014). The Privacy Engineer’s Manifesto. Getting From Policy to Code to QA Value. Page 251.

Stewart, J; Chapple, M; and Gibson, D (2015). CISSP(ISC)² Certified Information Systems Security Professional 7th Ed. Indianapolis,IN: John Wiley & Sons, Inc., page 160.

Dennedy, M; Fox, J; and Finneran, T (2014). The Privacy Engineer’s Manifesto. Getting From Policy to Code to QA value. Apress Open page 251 Stewart, J; Chapple, M; and Gibson, D (2015). CISSP(ISC)² Certified Information Systems Security Professional 7th Ed. Indianapolis, IN: John Wiley & Sons, Inc., page 662.

Maggie Gloeckle

VP of Privacy and Compliance Counsel

K Royal

Global Chief Privacy Officer

Crawford & Company

K Royal earned her JD from the Sandra Day O'Connor College of Law at Arizona State University. She also holds a PhD in Public Affairs from the University of Texas at Dallas.

Reach out to K about her column at @heartofprivacy on Twitter, or www.linkedin.com/in/kroyal/.