THE EXPERT'S VOICE® IN INFORMATION TECHNOLOGY

Managing Risk and Information Security

Protect to Enable

Malcolm Harkins

Apress open

Managing Risk and Information Security

Protect to Enable

Malcolm Harkins

Managing Risk and Information Security: Protect to Enable

Malcolm Harkins

formatting on specific devices, for all non-commercial purposes, in all media and formats known now or hereafter. While the advice and information in this Work are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

If your distribution is solely Apress source code or uses Apress source code intact, the following licenses (2) and (3) must accompany the source code. If your use is an adaptation of the source code provided by Apress in this Work, then you must use only license (3).

(2) **License for Use Direct Reproduction of Apress Source Code:** This source code, from ***Managing Risk and Information Security*** ISBN 978-1-4302-5113-2 is copyrighted by Apress Media, LLC, all rights reserved. Any direct reproduction of this Apress source code is permitted but must contain this license. The following license must be provided for any use of the source code from this product of greater than 5 lines wherein the code is adapted or altered from its original Apress form. This Apress code is presented AS IS and Apress makes no claims to, representations or warrantees as to the function, usability, accuracy or usefulness of this code.

(3) **License for Distribution of Adaptation of Apress Source Code:** Portions of the source code provided are used or adapted from ***Managing Risk and Information Security*** ISBN 978-1-4302-5113-2 copyright Apress Media LLC. Any use or reuse of this Apress source code must contain this License. This Apress code is made available at Apress.com/9781430251132 AS IS and Apress makes no claims to, representations or warrantees as to the function, usability, accuracy or usefulness of this code.

ISBN-13 (pbk): 978-1-4302-5113-2

ISBN-13 (electronic): 978-1-4302-5114-9

President and Publisher: Paul Manning
Lead Editors: Jeffrey Pepper (Apress); Stuart Douglas (Intel)
Coordinating Editor: Jill Balzano
Cover Designer: Anna Ishchenko

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com.

CHAPTER 3

Governance and Internal Partnerships

How to Sense, Interpret, and Act on Risk

> *If we are together nothing is impossible. If we are divided all will fail.*
>
> —Winston Churchill

To reduce cost, the company's human resources group wants to outsource payroll processing. At first glance, this might seem a low-risk decision. There's a clear business case, and outsourcing payroll doesn't create risks to

corporate information assets such as intellectual property. Most businesses regard payroll as a commodity application, so they might tend to select the supplier who can process the payroll at the lowest cost.

But there's more to consider. Employees' personal information will be transferred to the outsourcer, creating new privacy concerns. And imagine the impact if thousands of our employees don't get paid because the supplier experiences system problems on payday and lacks adequate disaster recovery capabilities.

Clearly, the HR group owns the business process. However, outsourcing payroll can introduce risks for the entire business, not just for HR. Payroll processes involve systems that can create information risk. Outsourcing also involves procurement. The business needs a clear overview of all the factors, including the risks, in order to make the best decision. To provide this view, the HR, procurement, and information risk and security groups need to work together.

A typical organization makes many decisions that require this kind of internal partnership to manage the risk. A product group wants to outsource development work to bring a product to market more quickly. A marketing team wants to engage a developer for a new social media initiative.

Similar considerations also apply to internal technology transitions such as OS and application

upgrades. Each new technology introduces new capabilities and risks. Often, the technology also includes features or options designed to reduce risk. By carefully analyzing the risk and security implications, including privacy and e-discovery considerations, we can help manage the risk of the transition, and we can often capitalize on the new features to improve the risk picture overall.

For example, when Intel IT was considering whether to migrate to Microsoft Windows 7, the information security team partnered with other groups in a broad evaluation of the OS. We identified several features that could improve security compared with previous versions of Microsoft Windows, and these security capabilities were an important factor in the decision to deploy Microsoft Windows 7 across Intel's enterprise environment (Fong, Kohlenberg, and Philips 2010).

The ability to make these decisions with an accurate view of risk depends on having the right organizational structure in place. In this chapter, I'll discuss two key aspects of this structure:

- *Clearly defined information risk governance*. Governance defines who makes decisions, who can block them, and who is allowed to provide input.
- *Strong partnerships*. Partnerships

between the information risk and security team and other internal groups are critical in forming an accurate view of risk and managing risk overall. Some partnerships are formally defined as part of the risk governance structure; others are informal relationships. These formal and informal partnerships are so important that I'll dedicate a large part of the chapter to them.

Information Risk Governance

The Massachusetts Institute of Technology Center for Information Systems Research (MIT CISR) provides a useful definition of IT governance that neatly encapsulates some of the benefits: ". . . A framework for decision rights and accountability to encourage desirable behavior in the use of IT. Governance identifies who will make key IT decisions and how will they be held accountable."

Information risk governance is the component of IT governance that enables the organization to effectively

sense, interpret, and act on risk. Information risk governance focuses on enabling the business while protecting the confidentiality, integrity, and availability of information—whether it is corporate data or personal information about employees or customers. Through partnerships between the information risk and security team and other groups, the organization can make tactical and strategic risk management decisions based on business priorities and a full view of the risks. We gather risk perspectives from across the organization and obtain buy-in to risk management decisions: a diversity of input leading to unity in decision-making.

To some people, the word governance may imply unnecessary bureaucracy, or perhaps even a dictatorial approach. It's true that any governance structure requires work to set up and maintain, but the value easily outweighs the administrative cost. When implemented well, a concise decision-making process can be a powerful mechanism for helping to achieve business objectives. Effective governance helps drive alignment and solid decision-making; it enables the organization to move more quickly while managing risk. As MIT CISR notes, "good governance is enabling and reduces bureaucracy and dysfunctional politics by formalizing organizational learning and thus avoiding the trap of making the same mistakes over and over again."

Research at MIT CISR shows that the more businesses leverage the structure, tools, and techniques of

governance, the greater the potential benefits. In fact, MIT CISR's work suggests that firms with effective IT governance enjoy profits that average at least 20 percent higher than their competitors (MIT CISR 2012).

However, leveraging governance doesn't imply slavishly following rules and procedures. A few years ago, I encountered an IT professional who was regarded by some people, including himself, as one of the best managers in IT. He rigorously based his project decisions on the prescribed practices and procedures, and gathered the correct metrics for reporting progress. Yet the projects he was responsible for generally turned out to be large, expensive failures. His obsession with correct procedures often impeded, rather than facilitated, the projects he was working on.

To use an analogy, if you gave the same recipe to a top chef and an average cook, would you expect them to produce exactly the same result? Probably not. Expert chefs don't simply follow the rules; they continually make adjustments using their senses and experience to achieve the best results. The temperature of a cooking surface is not exactly uniform, so a chef may move the pots until they're simmering just right. Fresh ingredients vary from day to day; the experienced chef is alert to the differences and tweaks the recipe and seasoning accordingly.

Like recipes, IT policies provide a valuable framework. However, their value lies in what we can

achieve by following the guidelines. Sometimes we need to make adjustments based on sensing changes in business needs. Otherwise, like the procedure-obsessed IT project manager, we may scrupulously adhere to the rules but fail to achieve the desired outcome.

This is one reason that partnerships are so critical. They provide channels for dialogue, helping us sense changing business priorities so that we mitigate risk based on those priorities rather than our preconceptions.

Without a governance structure that facilitates this dialogue, organizations may take too rigid an approach when applying controls to manage and mitigate risks. For example, some security groups try to ban the business use of social media due to the risks, but attempting to stop the use of external social media web sites is counterproductive and, in any case, impossible. At Intel, we have found it's more effective to embrace social media and shape the way that employees use it, as I'll describe in Chapter 5. This approach, developed in partnership with other internal groups, enables the organization to enjoy the benefits of social media while managing the risk.

Finding the Right

Governance Structure

It's important to find an information risk governance structure that fits the organization and the overall way IT is governed. As discussed in the sidebar and summarized in Table 3-1, MIT CISR has conducted some interesting research to identify IT governance archetypes (Weill and Ross 2000). These archetypes may be useful when thinking about information risk management based on how your own organization governs IT.

Table 3-1. *IT Governance Archetypes*

Style	Who has decision or input rights
Business Monarchy	A group of business or individual executives (CxOs). Includes committees of senior business executives (may include CIO)
IT Monarchy	IT executives
Feudal	Business unit leaders, key process owners, or their delegates
Federal	C-level executives and business groups; may also include IT executives. Equivalent of central and state governments working together
IT Duopoly	IT executives and one other group (for example, CxO or business unit leaders)
Anarchy	Each individual user

Source: Weill and Ross 2000

IT GOVERNANCE ARCHETYPES

As defined in Weill and Ross 2000, 59

The way an organization governs information risk management must mesh with its overall IT governance. There's no single IT governance model, but in the influential book *IT Governance*, researchers at Massachusetts Institute of Technology Center for Information Systems Research described several archetypal models based on deliberately provocative political archetypes.

These archetypes may be useful when considering how to implement a risk governance structure that fits the organization's IT governance style.

In practice, organizations may have shifted between different IT governance models over time—from an IT monarchy during the mainframe era, toward a feudal model or business monarchy as distributed systems emerged, then swinging back to a federal model as they recognized there's a role for centralized IT. With the adoption of cloud computing, some organizations are now moving toward a

business monarchy.

Further complicating the picture, organizations may simultaneously use multiple governance models for different aspects of IT: the enterprise network might be managed as an IT monarchy, while a business monarchy governs the systems that connect to the network.

If an organization's IT governance model already includes strong links between IT and business groups, the CISO may be able to leverage those existing linkages to build partnerships for managing information risk. This might be the case in organizations at which the governance model resembles the federal or duopoly archetypes described in the sidebar, with IT and business groups both directly involved in IT governance. If the organization more closely fits the IT monarchy archetype (IT is run as a centralized function with weaker links to business groups), the CISO may need to proactively establish new partnerships with business managers.

Intel's Information Risk Governance

At Intel, as at most large companies, risk is decentralized: at any one time, our company is planning or managing many technology-related initiatives and events across practically every part of the business. Therefore, we need decentralized risk management processes. But at the same time, we need a broad centralized view of the dynamic risk landscape.

Our goal is to implement a comprehensive and balanced approach to risk management. To achieve this goal, our approach includes a large number of risk management activities grouped into five broad focus areas, as shown in Figure 3-1: oversight, monitoring, engagements, operations, and strategic activities.

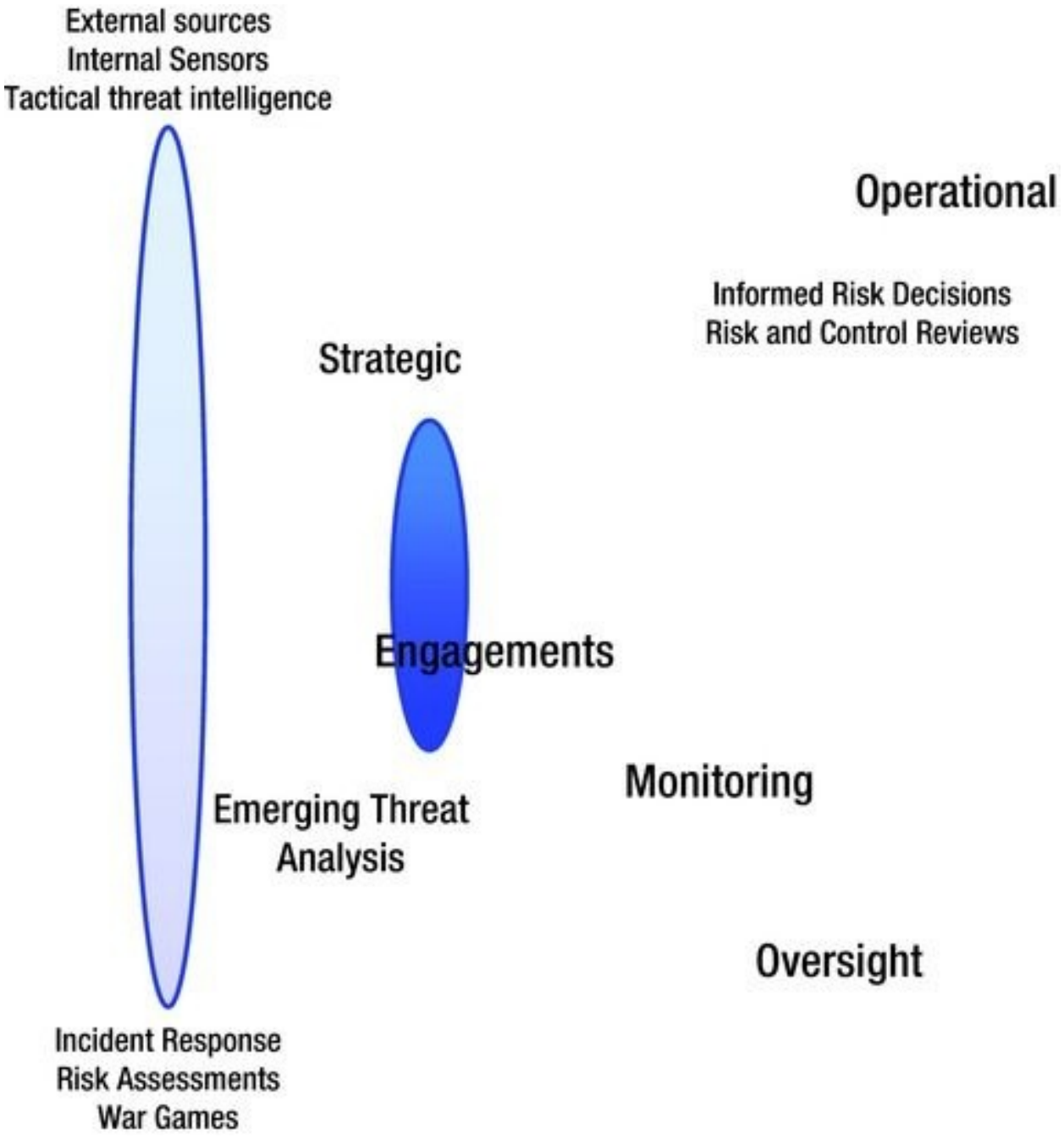

Figure 3-1. *How we manage the risks: Intel's internal information risk management focus areas. Source: Intel Corporation, 2012*

- *Oversight*. This area focuses on making informed risk decisions and reviewing risks. It includes committees and review

boards that set strategic direction, and review key risk areas such as ethics, compliance, and corporate investigations.

- *Monitoring*. We monitor (sense) risk through external and internal sources. External sources include industry research and analysis. Internal sources include internal partners who inform us of new business risks or legal requirements. These internal sources also include our own security technology sensors.
- *Engagements*. We participate in industry workgroups and in partnerships and dialogues with trusted peer organizations. These external engagements provide a valuable risk-sensing function and help us influence key security initiatives. I'll discuss our external partnerships in more detail in Chapter 4.
- *Operations*. This area encompasses day-to-day risk management activities and processes, including risk assessments, incident response, and exercises such as

war games.

- *Strategic*. Our strategic planning function interfaces with the other four components of governance. It includes our emerging threat analysis and long-range security architecture planning.

Our information risk governance structure is designed to support this balanced approach to risk management. It includes a large number of formal and informal partnerships and structures that help us sense, interpret, and act on risk. The partnerships also create a system of checks and balances by including diverse perspectives from different people across Intel, counteracting the inherent tendency for an individual group to introduce bias based on its own objectives (as I described in Chapter 2, we all have the potential to misperceive risk).

Building Internal Partnerships

By providing vehicles for dialogue and decision-making, internal partnerships enable information security teams to become more agile and responsive to business needs. The

number of potential partnerships has grown as the scope of information risk has broadened to include a range of privacy and regulatory concerns as well as traditional security threats.

Today, Intel's information security team partners with many internal groups for a variety of functions, including risk management decisions, incident response, and monitoring. These groups include legal, finance, human resources, and business groups.

Partnerships may include formal structures such as standing committees and risk review boards, as described in the information risk governance section of this chapter. We also maintain a large number of informal and ad hoc relationships. These are created and maintained through everyday communication with people in other groups. We might initially contact a business group to understand the potential impact of an emerging area of legislation. The business group identifies risks and opportunities that we hadn't even considered. Our initial request thus sparks a dialogue about requirements and controls, and ultimately evolves into a partnership that helps us monitor risks and mitigate them.

Whether formal or informal, these partnerships should be treated and managed as valuable relationships. Partnerships with other internal groups are essential in helping to build trust, as I'll describe in Chapter 9. We also gain business acumen, which helps us play a more

valuable role within the organization.

At Intel, partnerships have been critical to our success in understanding the broader risk picture, helping us sense, interpret, and act on risk. Through these relationships, other groups can act as additional eyes and ears for the information security group, helping us sense new risks, such as security threats and compliance concerns. For example, the HR legal group might alert us to an employment-related regulation that creates new compliance concerns. Information about risks flows in the other direction, too—we may alert our partner to new threats that we've encountered. As we leverage other groups to look out for our interests, they can also use us to look out for their interests. We also work with partners to interpret this shared information through analysis and decide how to act in response.

Establishing these relationships may create a far-reaching web of informal and formal partnerships across the organization. Although this web may appear complex, each partnership plays a role in helping us sense, interpret, or manage risk. Internal partnerships may focus on just one of the areas shown in Figure 3-1, or they may intersect multiple areas. For example, we partner with HR for incident response (operations), and to learn about new employment laws (monitoring). Multiple partnerships may also be required within each focus area: with the growing number of regulatory requirements, partnerships with internal groups such as HR legal, corporate security,

and internal auditing become increasingly important and valuable in the area of operational investigations.

Because no two organizations are identical, each organization may require a different set of internal partnerships, depending on its structure and business needs. Every partnership should be created with a clear purpose. The organization should also clearly define who is involved and who makes the decisions. To determine the partnerships your information security group needs, as well as their structure and purpose, it may be useful to ask the following questions:

- Who do we need to partner with and why? To put it another way, who do I interact with every day, and why do I interact with them?
- What benefits do I receive from that interaction, and what benefits does my partner receive?

In the remainder of this chapter, I'll discuss some examples of important partnerships, describing how we can use them and the value they provide. I'll start by examining partnerships with "fellow travelers" who have complementary roles in managing business risk and liability: legal, finance, human resources, corporate security, and corporate risk management groups. Then,

I'll examine partnerships with business group managers.

Legal

Legal groups are among the information security group's most important partners because of the many areas their roles intersect with ours. They own the responsibility for legal compliance and legal review. They interpret laws, analyzing the implications and relaying the relevant information to the rest of the organization. Key partnership areas include privacy, litigation, intellectual property, contracts, and compliance with financial regulations.

Privacy

As privacy regulations continue to grow in complexity and reach, many organizations need to comply with multiple requirements at local, regional, and national levels. Legal specialists across the organization can help us understand what's required in each geography, align policies and controls for protecting personal information, and decide how to manage responses in the event of a breach.

Even local regulations can have implications across the enterprise. For example, citizens of European countries

are subject to European and national privacy laws and regulations. The simple transfer of European employee personnel information to a US-based server will trigger a need to comply with the EU data privacy laws regarding such transfer of employee information.

Litigation

As one might expect, it's essential to partner with legal specialists in situations where litigation is possible or already in process. Examples are investigations of security breaches, particularly when law enforcement is involved. Another area of partnership is in responding to subpoenas and litigation discovery orders; a legal group may need to work with the information security team in order to collect the required information. To ensure that data is available for discovery when needed, we may also need to collaborate with the legal group to implement appropriate data retention policies.

Intellectual Property and Data Classification

Many organizations use a data classification structure to

protect intellectual property, with the most highly classified information receiving the greatest protection. We work with legal groups to specify the classification structure and then implement controls on management and distribution of such information to provide the appropriate level of protection. We also partner to respond to suspected or known IP thefts. Suppose an employee loses a laptop storing the designs of future products: a dialogue with IP attorneys is essential to understand the implications and decide how to respond.

Contracts

Almost every contract with a supplier or customer contains a confidentiality provision, which sets expectations about how each party will maintain the confidentiality of the business transaction and any shared confidential information. We partner with the procurement organization as well as the legal group to define and implement these requirements into contracts.

If our company decides to outsource a business application to an external supplier, we'll typically work with the procurement organization and legal team to define these confidentiality and data security expectations, as well as the evidence we'll need to validate that those controls are operating properly. For example, when hiring

a company to manage health benefits, we set expectations about how they must protect our employees' personal health information.

Our customers have expectations, too. A computer manufacturer may need to share some IP with us to help us integrate our technology into their product. We need to understand their requirements and ensure that appropriate controls are implemented.

Financial Compliance

In the United States and other countries, public companies are legally required to disclose "material events"—those likely to have significant financial impact that could affect investor decisions, including IT-related incidents. An important aspect of risk governance, therefore, is partnering with legal groups to understand the types of events and specific incidents that must be reported.

Guidance from the US Securities and Exchange Commission specifically discusses the obligation to disclose the impact of cyber attacks, including those that result in IP thefts. Companies are also required to disclose material increases in security spending in response to an attack, even if the attack didn't result in a loss of IP (SEC 2011).

The legal team cannot do this alone because it lacks

the security context of the event—the frequency of specific types of attack, the potential impact, and the cost of response. Therefore, the security team must be involved.

In 2010, Google disclosed that it had been breached in the widely publicized Operation Aurora attack. At around the same time, Intel also experienced an incident of similar sophistication. This was before the SEC issued its guidance in 2011, but as I pondered the potential ramifications of a cyber breach one sleepless night, I realized that I should call our SEC legal experts to discuss the incident. Subsequently, we disclosed the incident in our financial report for the first quarter of 2010 (Intel 2010).

Legal Specialists Within Business Groups

At large companies, each business group may have embedded legal experts. We need to work with them for issues directly related to their group. In addition, because of their connections within the group, these legal professionals can be extremely helpful in influencing the group's controls and expectations.

Marketing groups, for example, usually include individuals who want to explore new ways to

communicate with users via social media. This appetite for adventure is a good thing; it can benefit the business. But at the same time, we have to ensure that content is adequately protected and includes appropriate privacy protection and statements. If we bring up the issue directly with marketers, we may receive a lukewarm response, as they tend to view any controls as restrictions on their ability to move quickly. But the legal professionals within the marketing group understand the need for controls. So a good way to raise our concerns is to have a conversation with the business group's attorney, who can help persuade others in the group that controls are needed.

At Intel, we implemented a program that reviews all new externally facing online projects and monitors for potential problems (see sidebar). The projects may range from web sites to more sophisticated tools, such as an application that users can download and use in conjunction with external social media sites.

As part of the review, we ask the project group who their legal contacts are so that we can verify that they've received legal approval. We also ask whether trademark and branding teams have reviewed the initiative, which is essential in many cases—especially if the project is planning to register a new web site. Sometimes the answer is no, in which case we can facilitate a dialogue with the trademarks and brands team. This enables the trademark and brand people to manage the risk and helps

forge yet another important relationship within the company.

SECURING INTEL'S EXTERNAL ONLINE PRESENCE

Intel's business groups use hundreds of web sites and third-party solutions, including social media platforms, to communicate and conduct business with customers and business partners. Collectively, these externally facing Intel-branded solutions are known as Intel's *external presence*.

Until 2006, these web sites proliferated rapidly in response to business needs, without centralized oversight. Given this growth and following a number of security incidents and the identification of several significant risks, we established the Intel Secure External Presence (ISEP) program to provide appropriate security for Intel's external presence (Leon 2011).

The goals of ISEP, which is part of Intel's information security group, are to protect Intel's information assets and customers against threats such as loss of personal information and

malware attacks, and to maintain compliance with laws, regulations, and standards. By achieving these goals, we also help to protect Intel's corporate image.

We help ensure this protection and compliance by reviewing all planned new external presence projects and by monitoring existing Intel-branded web sites. ISEP review and approval is mandatory for new externally facing online projects. We work with Intel business groups to review planned projects before launch, whether they are to be hosted within Intel or by a third party.

The ISEP process includes several key aspects:

We make sure that we receive notification of new projects by working closely with business groups and other stakeholders within Intel. For example, we are notified when business groups request new Internet domain names or seek approval to land a new application in our externally facing IT environment.

For each project, we work with the business group to review details of the planned approach to maintaining security and privacy compliance.

We verify that the project includes any required mitigating controls before giving approval.

A key to our success is an overarching governance board, including senior managers from multiple Intel stakeholder groups. This board provides enforcement powers including the ability to shut down web sites for noncompliance.

We have applied the ISEP security review process to hundreds of new projects. In addition, we conduct daily vulnerability scans on all of Intel's externally facing web sites—more than 450—while maintaining a high compliance level with a vulnerability assessment standard based on industry best practices. Overall, ISEP has effectively helped secure externally facing Intel-branded web sites and solutions, resulting in a significant risk reduction for Intel's external presence.

Human Resources

The human resources group is the organization's center of expertise on employee procedures. HR may also include legal specialists who are the organization's experts on

employee-related laws. At some organizations, HR is also responsible for other functions, including internal and external communications. Because of this broad charter, the security team may form valuable partnerships with HR in several areas, including employee policies related to appropriate use and protection of information assets, internal communications, and investigations.

Setting Employee Expectations in Security Policies

Employees are part of the security perimeter, as I'll discuss in Chapter 5. Their behavior can have as much impact on security as the technical controls we use—particularly since a growing number of user interactions with the outside world take place on external web sites and networks, and on personal devices such as smartphones.

It is therefore critical to create employee policies that set expectations for secure behavior. If we can influence employees to behave in more secure ways, we can reduce risk for the business overall. However, the security team cannot write these policies without partnering with HR, including HR legal specialists, to ensure that they comply with employment laws and the organization's existing rules. Then, if an employee disregards the policies, we

need to work with HR to take disciplinary action.

Careless behavior can have highly damaging consequences. Imagine an IT employee who decides to store some corporate data on a server at his home so that he can more easily work on projects when out of the office. But his home system is open to the Internet, and thus the data may be broadly exposed to anyone worldwide.

The employee's action has created a significant security risk. To explain the potential impact to HR, it may help to use analogies. We could say it's like an engineer taking critical product designs home and showing them to her neighbors. Or a factory employee taking dangerous chemicals home to experiment with them, and creating the danger of an explosion in his garage. If we have a good relationship with HR, we can have this kind of discussion and determine the appropriate consequences for the employee.

Employee Communications

The responsibilities of the employee communications group often include employee training, employee awareness, and internal distribution of other corporate information. This group's expertise can be very useful when we want to communicate security messages to the

workforce. The group already has established communication channels and knows how to align messages with corporate style guidelines. A good employee communications group also knows how to present information in ways that engage employees rather than intimidate them.

At Intel, we work extensively with the employee communications group to create engaging security awareness messages, including interactive content that helps encourage secure practices when using social media and the Web.

Investigations

Partnership with HR is also essential in internal investigations. If it's an investigation initiated by HR, they may need our help to identify the information that may have been compromised, the implications, and possible responses. In other cases, we may already be pursuing an investigation and need help from HR legal specialists to access employee information.

Finance

The finance group typically takes the lead in managing risk and controls for the organization overall. Therefore,

we need to partner with the finance group to assess the business impact of damage to information assets—a loss of confidentiality, integrity, or availability. We also work together to determine the required controls.

Sarbanes-Oxley Compliance

The corporate finance team usually has overall responsibility for Sarbanes-Oxley (SOX) compliance, so we need to work with them to determine the appropriate controls. We must be able to attest to the financial integrity of our financial statements—to be sure the numbers accurately reflect our financial condition. This requires controls at all levels: within financial business processes, the applications, and the IT infrastructure. We also work with the finance group, as well as legal groups, to determine whether we should categorize specific events as material and report them as required by SOX.

Working with Business Groups

Each sizeable business group is likely to have a group controller or other financial specialist responsible for financial controls. These finance experts can become important partners for the security team.

Because financial specialists focus on risk and controls, the culture among finance specialists has some similarities with the culture of the information risk and security teams. This shared focus can make it easier for us to communicate our concerns, particularly since the impact of information risk is often measured in financial terms. Therefore, the financial specialist can be a key contact point when we need to discuss information risk with business groups.

Sometimes these risk conversations can evolve into productive multi-way partnerships. A recent example: an IT team presented plans for new systems to support one of Intel's new businesses. As we assessed the information risks, we noticed that the plan didn't include fully redundant systems to ensure business continuity. When we asked why, it emerged that the business group hadn't requested redundancy because it would add cost. Revenue from this new business was initially expected to be modest, so the group's budget was limited.

However, when we discussed the revenue projections with the finance specialists who worked on the project, they expected the business to grow rapidly. This growth would also increase the information-related risk because a system failure would have a much bigger impact on revenue. As we discussed the implications, it became clear that it would make more sense to prepare for the anticipated growth by including redundancy from the start. So we suggested that the business group negotiate a

higher budget—and that's what happened through a partnership between the business group managers, the information security team, and IT finance and business system specialists. The business group allocated increased funding that allowed IT to implement a redundancy safety net that would protect the growing business.

Internal Audit

Financial groups are often also responsible for internal audit, which typically includes an IT auditing function—a job with considerable potential for overlap with the information security group's role. If the security team and internal auditors duplicate each other's efforts, we'll waste resources and annoy business groups. Imagine if we contact a business manager to say that we need to conduct a risk evaluation of the group's systems. The next day, internal auditors contact the same group and say they're planning to do an audit, which some business managers might perceive to be essentially the same as a risk evaluation. What kind of reception do you think the auditors would receive?

We can minimize the overlap by partnering with internal auditors. This partnership becomes a mechanism for effectively allocating risk management resources. If the information security team has already assessed a

system, auditors may be able to increase the efficiency of an audit by leveraging the work that the security team has already performed.

For effective partnership, our work must be thorough, transparent, and well documented so that auditors can see what we have done. We may also swap resources: sometimes security experts may act as guest auditors for specific projects because they have skills that the financial group lacks. The partnership can also be used for valuable dialogue and mutual support. If we're concerned about a system that internal auditors have previously examined, we can ask for their opinion. We'll sleep better knowing that another group of objective, risk-focused specialists has analyzed the system.

Corporate Risk Management

Most large organizations employ people whose job includes purchasing insurance for general business risks, including property and casualty insurance to protect the organization in the event of damage to a data center or another facility. When buying insurance, the corporate risk management team may need information from us about the organization's IT business continuity and disaster recovery plans. Insurers ask for this information in order to set premiums.

Today, the corporate risk management team usually

focuses on physical risks. But their scope is rapidly expanding to include IT-related risks as well. Privacy breaches or other compromises can have a major impact on a company's revenue, cost, and brand image. Because of this trend, insurance against cyber risks is a rapidly growing category, and we can expect a growing need to partner with the corporate risk management team to ensure adequate coverage of information risks.

Consider the case of Sony, which suffered a breach of its PlayStation Network—estimated by the company to cost at least USD 200 million (Perlroth 2011)—and then became embroiled in a legal dispute with its insurer, which claimed Sony's insurance policy did not cover cyber risk.

Privacy

Privacy and security are closely linked. However, increasing security doesn't always enhance privacy. In fact, it can have the opposite effect. Unfettered monitoring of information and activities can increase security but intrude on personal privacy.

This creates inherent tension between security and privacy interests. This tension is apparent at a national level in the way that privacy advocates respond to the use of surveillance and data mining. Government security organizations may feel that they protect data extremely

well, but privacy advocates still object to the fact that information is collected and the way it is used.

Similar concerns apply at the enterprise level. We need to carefully manage the relationship between security and privacy, ensuring that we apply the appropriate level of controls to protect information without infringing on personal privacy.

The structure of this relationship varies between organizations. At Intel, the information risk group includes a privacy team that reports to the CISO. At other organizations, privacy is the responsibility of a separate group headed by a chief privacy officer who is the CISO's peer. This arrangement necessitates careful management of the relationship between security and privacy teams to manage tension, align policies, and control breaches. In organizations with this structure, the security team sometimes complains that the privacy team is "getting in their way"—which usually means that the security team wants to collect specific information and the privacy team objects.

Regardless of the organizational structure, it is the security team that is logically responsible for implementing IT controls. Laws define privacy rights; the organization's interpretation of those laws drives compliance requirements. It is the security team's responsibility to determine how to implement controls to support those requirements.

Corporate Security

The corporate security team focuses on physical security concerns—ranging from door locks and guards to break-ins, fires, and natural disasters. By partnering with this team, we can make sure we're aligned on protection of key information assets. It wouldn't make sense to implement sophisticated data-protection tools on the servers in the data center—and then leave the data center doors unlocked.

We also need to coordinate on other issues, including incidents that involve law enforcement. Not so long ago, assaults and harassment were almost always physical incidents handled by corporate security and the police. Today, there's a much bigger overlap with information security. More crime is moving online, and we may encounter other problems, such as cyber bullying. Because of these trends, we may need to help assess the impact and drive the response.

Business Group Managers

Each business group has its own processes and applications—whether it's a product-focused unit responsible for generating revenue or an internal group managing finance or human resources. The information

security team needs to partner with each group to implement security controls that protect the group's applications and information.

Direct relationships with business group managers and any risk management specialists within their groups, are invaluable for strategic and tactical reasons. By working closely with business managers, we can better understand their security priorities. As the business acumen of our information security team increases, we can better fulfill our "protect to enable" mission by focusing on controls that improve security without impeding the business.

By working with business groups, we can also leverage their strengths. Business group managers can help drive decision-making and incident response. They can also help improve security by setting the "tone at the top"—publicly setting expectations for their employees' security behavior. Suppose we notice that an increasing number of the employees at a specific facility are experiencing laptop thefts. We discuss the trend with the general manager and explain that we want to increase employees' awareness with messages about how to prevent theft. The business manager may offer to help by bringing up the topic at a site meeting or otherwise directly communicating with employees. This management request may exert a more powerful influence on employee behavior than messages sent by the security group.

HOW INTEL IT RESPONDS TO EMERGENCIES

Defining a clear IT incident response process is an essential aspect of IT governance. Over time, Intel IT has developed a clearly defined crisis management process for responding to emergencies and other significant incidents that affect IT infrastructure or services (Fleming and Tomizawa 2012). The goal of the process is to prevent material impact to Intel and its employees.

Incidents that may trigger the process include cyber events and other information security incidents; physical incidents such as fires, leaks, and major outages that affect IT systems; and major disease outbreaks. We developed the process using incident management principles based on the US Federal Emergency Management Agency's response to disasters.

Once initiated, the Intel IT Emergency Response Process (ITERP) operates with a command-and-control structure, led by an incident commander who has overriding authority to make decisions across IT for the duration of the emergency. The structure

consists of a virtual organization staffed on a volunteer basis by people from every discipline within IT. When an incident occurs, all team members perform their response roles instead of their normal duties until all issues are resolved.

Following an incident, we quickly identify the state of critical business processes that must continue during the crisis. We determine the current status of the key steps in our product cycle: design, build, order, ship, pay, and close. We assess the physical state of the infrastructure. We analyze the legal and other impacts if intellectual property or personal information is compromised. Decisions about response and remediation are driven by the incident commander and determined by business priorities.

The ITERP team has proved to be an essential component of the successful resolution of every crisis management, coordination, control, and communication activity in IT for the past 11 years.

Conclusion

Information risk has become a major concern for the entire organization. Managing information risk therefore requires a clear governance structure that enables the organization to make the right security decisions quickly and effectively.

Think about how your own organization manages information risk. Do you develop strategies in close collaboration with business groups? Do you feel that you communicate well enough with every group to understand their priorities and implement controls that reflect them? Have you clearly defined all the processes required to respond to a major breach or denial-of-service attack? If you answered “no” to any of these questions, you may need to improve your information risk governance.

Effective governance relies on partnerships between the information security team and other internal groups across practically every part of organization. In this chapter, I’ve described some of the most important partnerships and the value we can derive from them.

To develop these partnerships, CISOs need more than just technical skills. We need to communicate in terms business people understand and build relationships that enable us to influence people at all levels across the organization. As the scope of information security expands, we also need extensive management and leadership skills, both to operate at an executive level and to inspire our security team. I’ll discuss these skills in

detail in Chapter 9.