CHAPTER 4

External Partnerships: The Power of Sharing Information

Chance favors the connected mind.

—Steven Johnson

After spending a day at a conference, I was having dinner with a dozen or so peers when a debate began about the dangers and benefits of sharing security information with other companies. One person turned to me and asked me whether, if I had information about a specific new threat, I would share it with him.

"You bet," I said.

"But what if I was your competitor? Would you still share?" he asked.

"Our companies might compete for business," I replied, "but in the security arena, my real competitors are the malicious actors who want to harm my company's information systems. Those are my competitors, and they're your competitors, too."

As soon as I'd said this, several people at the table agreed. This agreement was gratifying—and not just because I felt that I had support for my views. The bigger implication was that my peers saw the value of sharing information outside their companies.

This hasn't always been the case. Historically, many organizations frowned on the idea of sharing security information externally, and more than a few had policies forbidding it.

However, attitudes are changing. Although there is still resistance at some companies, many organizations now see the value of sharing information and have begun doing so. Evidence includes the growth of industry-specific information-sharing communities, such as the retail-industry group that formed after Target's massive customer-information breach in 2013. There are also innovative partnerships that have a regional rather than industry-specific focus, such as the Arizona Cyber Threat Response Alliance.

Supportive actions by the US Government have also helped encourage information sharing. In 2014, the Federal Trade Commission and Department of Justice issued a policy statement indicating that sharing threat information was unlikely to raise antitrust concerns. This addressed a key reason that some big organizations had been reluctant to

M.W. Harkins, *Managing Risk and Information Security*,
DOI 10.1007/978-1-4842-1455-8_4

share information. “Cyber threats are increasing in number and sophistication, and sharing information about these threats, such as incident reports, indicators, and threat signatures, is something companies can do to protect their information systems,” said Bill Baer, an Assistant Attorney General in charge of the DoJ antitrust division (U.S. Department of Justice 2014).

In 2015, the White House issued a statement encouraging information sharing as a way to help safeguard national and economic security, and directing the Department of Homeland Security to support the formation of information-sharing groups under the umbrella term Information Sharing and Analysis Organizations (ISAOs). And in 2015, legislation was proposed to promote sharing of threat information, although the effort stalled in Congress.

Despite the overall shift in attitude, some organizations still have reservations about sharing information. There are three major areas of concern. First, organizations worry about the legal and regulatory implications of revealing information about threats. A second, related concern is the public relations aspect. Both of these fears have a valid basis. Information security has become an enterprise risk management issue of board-level interest because of the potential effects. Information leaks revealing potential intrusions and data breaches can have legal consequences: the organization may be required to report the problems in order to comply with financial and privacy regulations, for example. If security issues become public, they may also damage the way the organization is perceived by customers and by the business community, potentially affecting a company’s profitability and its stock price. The third major area of concern is privacy. This also has a valid basis. For example, sharing information that identifies the victim of an attack, as some security specialists would like to do, clearly can expose machine data that can potentially compromise the victim’s privacy. Some people also see a risk, following the revelations of National Security Agency eavesdropping, that legislation could be used to enable government surveillance. For these reasons, I believe that any cybersecurity legislation must include appropriate privacy protection.

What’s the payoff from sharing information? My personal experience is that I have obtained real value: information shared by others has helped me understand threats and take action. I have also seen that it’s possible to share useful information while avoiding the issues mentioned above. Companies can share information about attacks without revealing personal information about the victim. They can share indicators of compromise without revealing confidential information. They can alert other trusted contacts during the early stages of investigating a threat, before it’s been determined whether a compromise has occurred that requires regulatory disclosure.

The growth of information-sharing groups shows that many other organizations now share my belief in the value of sharing information about threats and best practices. As I’ll explain in this chapter, sharing security information can provide considerable benefits in managing the risk of moving into new business relationships and adopting new technologies. We just need to find ways to reduce the risk of sharing. The solution lies in creating trusted information-sharing relationships with other organizations. The more we trust the relationship, the more sensitive the information that can be shared.

The need to share security information is being driven by rapidly changing business, technology, and threat landscapes. Increasingly, companies are collaborating with a broad variety of business partners. We share business information, and often we also use the same technology, or we sell or share technology with each other. As we do so, we also share risks. Understanding the risks faced by our partners, and the way they manage those risks, can help us protect our own organizations.

Looking more broadly across the technology landscape, all systems and devices are to some extent connected, whether they are owned by enterprises, individuals, or service providers. Almost every aspect of society depends on a worldwide, rapidly evolving, highly complex network of devices and services. This provides the central nervous system that supports innovation, economic development, and social interaction worldwide. But because we are all inherently interconnected, we share common risks. The threat landscape is dynamic, global, and increasingly complex. Threats may originate in any country and then spread rapidly across national and enterprise boundaries, causing extensive damage to organizations and individuals worldwide.

Because threats spread so quickly and the threat landscape is so complex, it is hard for any single organization to gain a clear view of all potential vulnerabilities, threats, and attacks. External partnerships can help. They provide additional intelligence that we can use to improve our own security posture. By exchanging information with other organizations, we gain what I call *outsight*, or a better understanding of what happens outside our own environment. We learn about new threats before they hit us directly. We see how other organizations are managing those threats. We learn about best practices for managing security operations. Using the information we gather from external relationships, we can increase the organization's ability to sense, interpret, and act on risk.

The Value of External Partnerships

Sharing security-related information can require initiative and courage. The idea of sharing information externally may run counter to the culture of the organization overall, including the culture within the security group. Organizations may view security information as proprietary and confidential, like intellectual property. Many still have policies against sharing information.

It's true that much security information is sensitive, and sharing it can introduce risks. Because of this, we need to be careful about what we share and with whom.

But think about the broader context of how organizations are increasingly sharing information. Most organizations have already recognized that they need to share sensitive business information with partners in order to develop, manufacture, and market new products. Collaboration with other companies is becoming an integral part of many other business processes, too. As organizations share information, they benefit from their partners' insights and expertise. As noted by Steven Johnson, author of *Where Good Ideas Come From: The Natural History of Innovation* (Riverhead Books 2010), many of the best ideas have emerged not through the inspiration of a single mind, but through the exchange of ideas. "You have half of an idea, somebody else has the other half, and if you're in the right environment, they turn into something larger than the sum of their parts," Johnson said in a speech at the 2010 TEDGlobal conference (Johnson 2010). "We often talk about the value of protecting intellectual property—building barricades, having secretive R&D labs, patenting everything that we have, so that those ideas will remain valuable … but I think there's a case to be made that we should spend at least as much time, if not more, valuing the premise of connecting ideas and not just protecting them."

I believe that there's similar value in sharing security information. As we collaborate with business partners, we need to understand the threats to their environment, and how they manage risk, in order to determine what we need to do to protect our own organizations. Each partner in a value chain needs to protect information to a level

that is adequate to protect the other partners; the weakest link in the chain can impact everyone. Note that throughout this chapter, I use the terms "partner" and "partnership" in the colloquial sense, not to imply any specific type of formal legal relationship.

There are many other examples of how sharing information can benefit all organizations involved. If we are entering new markets through business partnerships, we need to understand the nature of the threats in those markets from the companies currently operating there. The same logic applies to using new technologies. Organizations are extending their environment to customers and becoming suppliers of mobile apps and web services in the process. As they do, they can learn from other companies' experience how to manage the risks. Companies are increasingly sharing cloud capacity or other data-center infrastructure supplied by external providers, and can all benefit by sharing feedback with the provider about risks within the environment.

Despite these trends, some organizations still have policies stipulating that employees shouldn't share internal information about risks and threats with anyone outside the company. This is sometimes the case even when the same organization willingly shares other IT-related information such as helpdesk or e-mail management best practices.

Without wishing to discount the real fears driving these policies, the value of sharing information often outweighs the risk of doing so. Let's imagine that a CISO learns of a new threat affecting companies in his industry sector. He shares information about the threat with a peer at another company and, by doing so, gains insight that helps the organization mitigate an attack that has caused massive damage at other companies. By sharing information against company policy, the CISO took a personal risk. Yet by doing so, he averted the bigger risk of business disruption and damage to the organization's reputation.

Failure to share information with others introduces its own risks. If we don't share with peers, they won't share with us, so we won't benefit from their information and insights. I've seen cases in which information security professionals wanted to participate in communities, but weren't allowed by their companies to share any internal security-related information. So they attended meetings but couldn't contribute. Ultimately, their peers wouldn't tolerate a situation in which these people were receiving information but giving nothing in return, and they were effectively voted off the island.

External Partnerships: Types and Tiers

Much of the publicity about information-sharing initiatives has focused on public-private partnerships related to critical infrastructure and national security. However, there are many other types of formal and informal external information-sharing relationships, including 1:1 partnerships and groups comprised solely of private-sector organizations.

External partnerships are most often used to share information about specific threats and best security practices. But some partnerships focus on other types of information. For example, security specialists within the high-tech sector share information in order to develop security standards, which are then implemented in various products.

Much of this security information is sensitive. Because of this, we need to be able to trust that the partners with whom we share information will treat it appropriately. The more sensitive the information, the greater the level of trust required. In general, the level of trust can be higher in relationships with fewer people, allowing more-sensitive information to be shared. As the number of people increases, there's a greater chance that information will leak, so the level of trust tends to decrease and only less-sensitive information is shared.

Relationships therefore naturally tend to fall into a tiered pyramid model, as shown in Figure 4-1 (Willis 2012). At the top of the pyramid are the most-trusted relationships with the fewest partners; these are 1:1 partnerships between two individuals at different organizations, or between two security teams.

Information-sharing relationships between more than two partners are often referred to as communities. Because more people are involved, a legal or peer-enforced agreement is usually needed to define the level of trust and confidentiality expected among community members.

The two middle tiers of the pyramid include groups with intermediate levels of trust, sharing information with varying levels of sensitivity. The *targeted tier* typically consists of public-private partnerships aimed at protecting critical infrastructure. The *confidential tier* includes many private-sector communities, including regional communities and those focused on specific industry sectors.

At the bottom of the pyramid is the *public tier*, comprised of the largest communities with the lowest level of trust. At this level, information is often public and may be broadcast via the Internet. This tier might include groups that develop educational information about threats for public distribution, or CISOs who share their insights via public webcasts.

I should note that there is considerable overlap between these tiers. A group may have characteristics of both the targeted and confidential tiers, for example. Also, the number of members in groups within each tier (shown in Figure 4-1) is just a guideline: communities at all levels tend to grow over time as more organizations see the value and join.

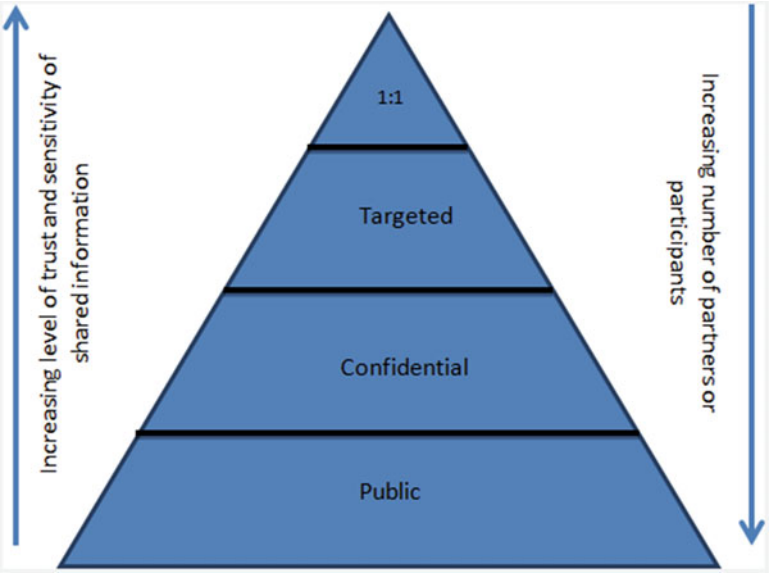

Figure 4-1. *Tiered pyramid model for trusted information-sharing partnerships and communities (adapted from Willis 2012). Source: Intel Corporation, 2012*

How can you get involved in information-sharing partnerships? One good method is to start by participating in communities in the public tier, where the information shared has a relatively low level of sensitivity and therefore involves little risk. In these communities, you're likely to meet peers with whom you can begin to engage in 1:1 partnerships. As you become more knowledgeable about the communities that reflect your organization's key interests, you may then become involved in relationships in the middle tiers of the pyramid, where more confidential information is exchanged. I have always made sure that my teams and I actively participate in partnerships at all the tiers of the pyramid.

1:1 Partnerships Tier

- **Community structure**: Direct communication between CISOs at two organizations or between their teams
- **Typical number of partners**: 2
- **Example partnership/community**: Any two organizations who choose to share information
- **Example goal**: To mitigate shared threats by exchanging information with a business partner more quickly and in greater detail than would be possible within a larger group
- **Trust framework**: Personal trust and existing business relationships

Targeted Tier

- **Community structure**: A relatively small number of critical information infrastructure owners and operators sharing information to protect the infrastructure. Also includes key security ecosystem influencers, such as large security service providers or vendors.
- **Typical number of partners**: Up to about 50
- **Example partnership/community**: Information Sharing and Analysis Centers (ISACs)
- **Example goal**: To prevent advanced persistent threats (APTs) within the industrial base by sharing APT signature information
- **Trust framework**: Strong information-sharing frameworks, such as national security clearances and nondisclosure agreements, are required. Trusted sharing mechanisms, such as encrypted web portals with multifactor authentication, are also required.

Confidential Tier

- **Community structure**: Communities that represent industry sectors or other groupings, such as the banking sector and Internet service providers (ISPs), or regional forums
- **Typical number of partners**: Up to about 100

- **Example partnership/community**: BITS (financial services industry), Bay Area CSO Council (regional), Regional CSO Summits
- **Example goal**: To enable members to protect against common threats and vulnerabilities affecting their industries. For example, ISPs might share the command and control Internet addresses that botnets use.
- **Trust framework**: Communities typically use trust frameworks such as nondisclosure agreements or memoranda of understanding.

Public Tier

- **Community structure**: A broad range of communities that represent all user categories, including consumers, small- and medium-sized businesses, and industry in general
- **Typical number of partners**: 100s to 1,000s
- **Example partnership/community**: Forum for Incident Response and Security Teams (FIRST), National Cyber Security Alliance
- **Example goal**: To share best practices or informational bulletins about widely known threats and vulnerabilities that affect a large cross-section of users.
- **Trust framework**: Trust frameworks are not necessary; communities typically distribute information broadly through mechanisms such as e-mail distribution lists or public web sites.

Let's look at these tiers in more detail.

1:1 Partnerships

In my experience, 1:1 partnerships are some of the most valuable security relationships. They may be formal or informal, established at a corporate level or between individuals.

As I explained, a key advantage of a trusted 1:1 partnership is that we can more safely share highly confidential information. We can often create a stronger bond with a single individual than with a larger group. As a result, the shared information often has a depth and richness that's lacking in information shared within larger communities.

Another advantage is speed. Communication is often fastest in 1:1 partnerships, partly due to logistics. It's much easier to set up a meeting between two people than it is to organize a meeting with a dozen people. To exchange information about the latest developments, a CISO may be able to simply pick up the phone and have a conversation with his or her peer. Quickly sharing information enables a faster response to threats—and in the security arena, timeliness is often critical.

Here's an example showing how 1:1 partnerships can develop and benefit both partners. Through my participation in a larger security community, I got to know the CISO at a fast-growing e-commerce company whose customers were primarily consumers. We both would contact each other periodically for advice and information as we puzzled over the latest security challenges. Over time, these conversations evolved into open dialogues about best practices and benchmarking.

The relationship eventually evolved to a point where we both realized we could learn a great deal more by bringing our teams together in a face-to-face meeting. The resulting half-day meeting proved incredibly valuable to both teams. Our team was able to provide insights and experiences about managing security in a large, complex enterprise environment. This was helpful to the security team at the fast-growing e-commerce company, which was in the process of building an enterprise environment to support its fast-growing business. In return, the team at the e-commerce company was able to share the security challenges and experiences of operating a large consumer business with millions of online customers. This was extremely valuable to us at Intel because we were in the process of expanding our external online presence and were beginning to encounter some of the same challenges.

The partnership thus expanded from ad hoc conversations to a productive relationship between teams sharing experiences and best practices at multiple levels. It's hard to imagine that this extensive information exchange could have occurred within a larger community.

Another example: I met the CISO of a large manufacturing company at an industry event, and we stayed in touch through occasional e-mails. Then, during a period of especially large-scale industry attacks, our communications suddenly became much more frequent and detailed. It was extremely valuable to be able to pick up the phone and simply call a peer to share the latest knowledge about the attacks and responses.

I have frequent 1:1 meetings with peers at other companies, sometimes as often as several times a week. These meetings can serve several purposes. A few years back, I met with a team from a key supplier to discuss our strategy for securing employees' personal (bring-your-own) devices. I shared our best practices with this team, and during the question-and-answer discussion, team members also provided information about how they were addressing the same problem. The meeting served as a helpful benchmarking exercise for all of us.

At the same time, the discussion clearly demonstrated each company's commitment to protecting its partner's business information. It showed the depth of each company's strategy for protecting information—revealing a commitment that extended far beyond the desire to comply with contract confidentiality clauses. I felt more confident that if a security issue ever arose, I could talk directly to my counterparts at the supplier company because their commitment to protecting information would enable a productive approach to resolving problems.

Another recent discussion, this time with a potential customer, focused on the cloud. The organization was concerned about our use of the cloud as part of our infrastructure, and also as a part of the service connected to our product. Rather than respond to the lengthy survey they had put together, we met with them to discuss how Cylance uses the cloud and which data we store there. We discussed the risks that could exist in the cloud infrastructure, the potential implications of those risks, and how we manage those risks. We also discussed other precautionary steps the customer could take to further mitigate the potential risks. This discussion helped develop a relationship that built the most customer trust.

Communities

Participating in larger communities may not provide information that's quite as rich and deep as the information you'd obtain from a 1:1 partnership with a peer. But communities provide value in other ways.

Because they contain more people, communities provide breadth and diversity of perspective that help us make balanced risk decisions. With a larger number of participants, there's a better chance that one of them will have developed a solution to a problem, or can provide valuable new information about an industry attack.

Some communities focus on sharing threat-related information; others on benchmarking and best practices, influencing legislation, developing security standards, or public education.

Communities can also present great networking opportunities. Through participation in communities, I've met several people with whom I've subsequently developed closer 1:1 partnerships.

Community Characteristics

Like all groups, communities require a structure and a set of ground rules to be effective. Successful communities typically have the following characteristics:

- **Clear goals**: The community shares clearly defined common goals that benefit members, such as mitigating an industry-wide threat. A community may have several goals.
- **A strong framework of trust, such as a legal or peer-enforced agreement, that addresses risks related to information sharing among community members**: For example, the Industry Consortium for the Advancement of Security on the Internet (ICASI) has a strong multilateral nondisclosure agreement, while other communities, such as the Bay Area CSO Council, rely on a peer-enforced trust framework.
- **Trusted communications channels**: Members can safely contribute and access shared information using an effective trusted communications channel or mechanism, such as a secure web site. These channels are not always electronic; some regional groups conduct face-to-face meetings to further reduce the risk of compromise.

An organization is most likely to benefit from joining communities if those communities align with the organization's security goals. This means it's important to first clearly define those organizational security goals. To do this, some organizations have found it helpful to use a structured approach; they can more clearly categorize their goals by mapping them to a standard risk management model, such as the "defense in depth" model. Once an organization clearly understands its own security goals, it can identify communities whose objectives align with these goals.

Because there is such a diverse range of organizations, security threats, and goals, it is unlikely that any single information-sharing community structure meets all the needs of a large organization. For example, a company might participate in one community for benchmarking and another to tackle industry-specific threats.

Information-sharing communities thrive only when the participating organizations feel they're receiving valuable information, creating incentives to continue to share information with others.

What constitutes valuable information? A common definition is that information should be timely, specific, relevant to participants' concerns, and provides a suitable level of detail while protecting individual privacy (ENISA 2010). In practice, "valuable" usually means the information helps you achieve your security goals, whether those goals are long-term and strategic, or short-term and operational. Information useful for strategic goals might include an early warning that attackers are expected to target a specific industry. This helps members of the community plan their defenses. Information useful for operational goals typically includes more specific details, such as an attack signature. This helps organizations more quickly identify an attack and respond when it occurs.

As shown in Figure 4-1 (the targeted tier), some communities consist of government agencies working alongside an industry in what are usually known as public-private partnerships (PPPs). These PPPs can be particularly important for protecting critical information infrastructure. Internationally and within many nations, this infrastructure is largely owned and operated by the private sector, including carriers and network service providers. Sharing information about threats and attacks among public and private agencies therefore can help ensure security and resiliency of this infrastructure. Because the shared information is highly sensitive, these PPPs usually have strong trust frameworks including national security clearances.

An example of a much broader public-private community is InfraGard, a partnership between the FBI and private- and public-sector sector organizations that shares information and intelligence to prevent hostile acts against the U.S.

Other communities are primarily comprised of private-sector organizations. Some are industry-specific: members of an industry get together to share threat information and best practices, helping to reduce risk for each company while enhancing the industry's reputation overall. Others involve sharing across industries, such as Evanta's CISO Coalition, a cross-industry group of executives from large organizations. The Coalition is designed to facilitate secure, real-time interaction among members to vet critical information security issues, and then share best practices for resolving them. As a part of my efforts to expand my external partnerships, I was fortunate enough to become a founding member of this group's advisory board. Another cross-industry group is the Security Advisor Alliance, a cybersecurity nonprofit dedicated to aligning CISOs to help one another, supporting the information security community (including startups), and giving back to schools and nonprofits.

Some communities are regional, aimed at security professionals from private and public-sector organizations located within a specific area. These regional communities offer the advantage of convenience. It takes less time, effort, and expense to attend a regional event, which makes participation more attractive. Examples of regional groups and forums include ACTRA (see sidebar) and the San Francisco Bay Area CSO Council, described shortly.

New communities arise frequently. A community may form in response to a specific threat because companies are strongly motivated to share information about the threat in order to develop effective defenses. For example, the Conficker Work Group was formed specifically to address the risk posed by the Conficker worm.

ARIZONA CYBER THREAT RESPONSE ALLIANCE

Innovative new models for information-sharing communities are springing up as the value of sharing security-related information becomes more widely recognized. An example is the Arizona Cyber Threat Response Alliance, Inc., a regional public-private partnership. This cross-sector group shares information about threats and other issues among partners from industry, academia, law enforcement, and intelligence.

ACTRA grew out of relationships developed with FBI's InfraGard, the public-sector Arizona Counter Terrorism Intelligence Center (ACTIC), and the U.S. Department of Homeland Security. A key difference is that ACTRA is a nonprofit company with a full-time president in addition to voluntary participants including a board and technical subject matter experts. The goal is to improve security for members with a flat, responsive organizational structure and without adding a burdensome layer of process. The group disseminates information ranging from alerts in near real time to white papers that provide insights and highlight best practices. ACTRA has grown to include representatives from 14 critical infrastructure sectors. The group has found, based on discussions with its members, that multi-sector sharing improves threat visibility beyond the single-sector focus of industry-specific groups.

Community Goals

Communities may focus on narrowly defined goals, such as mitigating a specific threat, or they may have broader information-sharing goals, such as benchmarking security techniques. A single community may pursue several goals. The most well-known types of goals are sharing information about threats (to help member organizations mitigate those threats) and sharing best practices (to improve efficiency). I'll describe sharing goals next.

Sharing Information about Threats and Vulnerabilities

Perhaps the best-known function of communities is to provide a trusted mechanism for sharing information about threats and vulnerabilities. Members of the community can use this information to improve their tactical and strategic situational awareness.

I'm often asked by peers how I measure the value of the information obtained from external partnerships. A key metric is whether the early threat information has helped enable us to reduce risk. A single piece of information might make participation worthwhile if it helps us better mitigate risk and protect the company.

Information from the community can also be useful for corroborating evidence that we've already identified internally. If we observe a potential new threat within our environment, we may not feel that we have enough evidence to justify taking action. But we can often discuss the issue within a community. If others are experiencing the same problem, we can be more confident that it's a real issue. This gives us enough reason to act.

Some examples of communities that share threat information include

- **Information Sharing and Analysis Centers (ISACs)**: ISACs are trusted industry-specific communities established by owners and operators of critical infrastructure resources. ISACs exist for a number of industry sectors, including communications, retail, electrical utility, health, and public transit. Services provided by ISACs include risk mitigation, incident response, and alert and information sharing.
- **Bay Area CSO Council**: This is a regional community that focuses on improving the sharing of intelligence and best practices among CISOs in the San Francisco Bay Area. The Council serves as a vehicle for CISOs to safely and securely share their attack experiences. Members may share artifacts, such as attack signatures, that they can then build into their organizations' detection and defense mechanisms (Jackson Higgins 2010). The forum uses a peer-enforced trust model rather than a formal legal framework. The group also creates subgroups to work on more highly classified information.

Sharing Best Practices and Benchmarking

Many communities also serve as a forum for exchanging best practices and for benchmarking operations. By sharing security best practices, we may be able to increase the efficiency and effectiveness of our own operations.

Tapping into the expertise of others can help us avoid reinventing the wheel. A typical example: A CISO is trying to create a bring-your-own device policy for her own organization. So she sends a message to community members and receives detailed advice from others who have already been through the process. This gives the CISO a head start in creating a policy that meets her organization's needs.

Besides enabling informal exchanges, communities may also operate formal benchmarking exercises. Some of the best-known examples are the security-related programs run by benchmarking firm CEB, Inc., which conducts studies and generates reports that compare companies in a variety of areas, from user security awareness to controls maturity (CEB 2015; also see the discussion of security awareness programs in Chapter 5). Benchmarking information generated by communities can also be useful for demonstrating the efficiency of security operations to other internal groups within your organization, such as an audit committee.

Some benchmarking information is sensitive and closely held because organizations feel that it could reveal too much information about their security operations. Other information is more general and is sometimes publicly available, such as the webinars and presentations published online by Intel and others. Even this general benchmarking information may yield risk insights. Observing what other companies are focusing on, and how they are allocating resources, can help security professionals think about how they need to manage risk within their own organizations.

One of the most established communities is the Forum for Incident Response and Security Teams (FIRST). This international group focuses on sharing best practices among computer security incident response teams. Trust relationships are peer-enforced. The group publishes a series of detailed best-practices guides and other documents for public use. Other activities involve the exchange of information for cooperative incident management.

Technology is helping to make information exchange more automated and therefore easier and faster, due in part to the adoption of standards for representing (STIX) and communicating (TAXII) information about threats. Platforms are emerging that use these standards for rapid, secure information sharing.

BENCHMARKING: WHO SHOULD YOU COMPARE YOURSELF WITH?

Many years ago, I was asked to manage Intel's first major IT benchmarking activity. It was a big task that entailed analyzing cost, quality, and other aspects of operations across our entire IT environment.

One of the first challenges was determining which organizations we should benchmark ourselves against. At the time, the conventional wisdom at most organizations was that you should compare yourself with similar businesses. The logic was that because these businesses were the most directly comparable, this approach would yield the most meaningful results. So the expectation was that I'd benchmark our operations against a collection of other big high-tech companies.

But I didn't want to benchmark our operations against only high-tech companies. Instead, I wanted to benchmark against a broad base of companies in industries such as retail, banking, manufacturing, consumer goods, and utilities.

The time came to present my selection of peer groups in a meeting with senior IT management. By this time, I'd already started the benchmarking process, and as I described the diversity of the companies included in the benchmark comparison, I could sense the atmosphere becoming increasingly hostile. Practically everyone felt that my approach was completely wrong. In fact, if there had been rotten tomatoes in the room, a few people would have been throwing them at me.

So I asked for a moment of quiet so that I could explain. If we were an airline that wanted to benchmark operations, who would we compare ourselves with?" I asked. Several people said they'd benchmark against other airlines.

"What do you think we would learn from that comparison?" I continued. "My guess is not much. We'd all have grown up in the same industry, and we'd probably have similar business processes. Many of our employees would have worked for the other companies and vice versa, so they'd probably implement similar practices. We might learn about minor efficiency improvements, but I wouldn't expect any breakthroughs."

> "If I really wanted to dramatically improve the way I manage airline gate operations, I'd benchmark against a Formula 1 pit crew. Those crews can service a car and get it back on the road in 20 seconds or less. I'd think about what we could learn from studying their processes, their technologies, and their ability to communicate and organize, and I'd try to figure out which aspects could cross over into airline data operations. If we want to make dramatic improvements, we need to look at people who operate in an extreme operational environment—not at other airlines."
>
> I'm happy to say that the managers in the room recognized that there might be value in the approach I was suggesting, even if many of them still disagreed with it. Ultimately, benchmarking against companies in a broad range of industries did help us achieve some dramatic improvements, and I received an internal award for the initiative. The lesson is that sometimes we can learn more by looking outside a narrowly defined, traditional peer group. People in the same industry may be facing the same problems as we are and dealing with them the same way. For a fresh perspective, it can be worth looking farther afield.

Influencing Regulations and Standards

All of us operate within an increasingly complex regulatory environment, and we're all affected by evolving technology standards.

It's important to stay abreast of legislative developments. That can be a difficult and time-consuming job for any single organization, and so it may be helpful to become involved in a community whose goals include tracking regulatory activity.

In addition, communities can sometimes help influence public policy more effectively than a single organization can do alone. There's strength in numbers, and communities often include some of the biggest companies in an industry.

An example of a community that focuses on policy is BITS (www.bits.org), the technology policy division of The Financial Services Roundtable, which represents 100 of the largest integrated providers of consumer financial services. Members of BITS cooperate on issues such as critical infrastructure protection, fraud prevention, and the safety of financial services. The organization works to influence public policy by communicating with public agencies. It also publishes reports for use across the industry, including a financial services security assessment. Thus, communities that focus on policy may help all participating companies and the reputation of the industry overall.

Businesses who offer services in multiple countries have a particular interest in the international regulatory environment. These include multinationals, of course, which are directly affected by the complex web of regulations at international, national, and local levels.

However, these regulations affect a surprisingly large number of other companies, including many that don't have employees or facilities physically located in other countries. Today, almost any business with a web-based service consumed in multiple countries is effectively operating in a multinational environment. Regulations in those countries have impacts that stretch beyond geographical boundaries. For example, regional and local regulations such as the California data breach bill (SB1386) and European privacy guidelines require compliance by any company that stores information about residents of those areas, no matter where the company is located.

Corporate Citizenship

At many companies a large number of employees volunteer in ways that benefit their neighborhood or a wide variety of worthy causes. Businesses often provide support to help employees do this. There's a growing trend to leverage the organization's talent and expertise in volunteer corporate citizenship initiatives that are more closely related to the organization's goals and employees' technical expertise. Examples might include offering expert security advice to nonprofits or helping security initiatives in other countries.

Security-related corporate citizenship initiatives include the National Cyber Security Alliance, whose mission is to educate and empower society to use the Internet safely and securely (see `staysafeonline.org`). The sponsors of the alliance include large high-tech companies such as Intel. Senior managers at those companies also are among the directors of the organization.

Conclusion

The knowledge we acquire via external partnerships can help us protect our own organizations. I've experienced this first hand; indicators of compromise shared by others have helped me understand and respond to threats. The growth of information-sharing groups shows that many organizations are coming to the same conclusion. As Ken Athanasiou, Global Information Security Director at American Eagle Outfitters, said in a statement supporting the formation of the new retail ISAC: "Cyber-criminals work non-stop, and are becoming increasingly sophisticated in their methods of attack … by sharing information and leading practices and working together, the industry will be better positioned to combat these criminals" (Retail Cyber Intelligence Sharing Center 2015).

Industry-specific groups such as the financial and industrial control ISACs have been widely acknowledged as helping companies quickly learn about threats and specific measures for combating them. Other groups provide different kinds of valuable information. The Evanta CISO Coalition has published metrics that its members can use for security benchmarking and dashboarding. Members of IASAP share information that helps them improve their awareness programs.

The security landscape has become increasingly complex and dynamic, and it's difficult to track and manage the risks without help from others. Sharing security information is also becoming more important as organizations increasingly collaborate with business partners and adopt new technologies. Understanding the risks faced by our partners, and the way they manage those risks, can help us protect our own organizations. As businesses move into new markets and use technology in new ways, we need to understand our biggest exposures and how to allocate resources most effectively to minimize business risk. Therefore, sharing information can help businesses remain competitive and successful.

Organizations have often been reluctant to share security information, but if we want help from other people, we have to be prepared to share information ourselves. By carefully using trusted partnerships that align with our security goals, we can increase our organization's ability to sense, interpret, and act on risk.