Protecting the Perimeter

ABSTRACT

At Intel, we are well aware of the risks associated with social media, but attempting to stop the use of external social media web sites would have been counterproductive and, in any case, impossible. We realized that if we did not embrace social media and define ways to use it, we would lose the opportunity to shape employee behavior. In general, people are likely to take better care of their own possessions than someone else's. They feel a stronger connection to their own car than to one provided by their employer. We found social media does not create new risks, but can increase existing ones. Recognizing this, we created policies and training tools, then deployed internal social media capabilities, such as wikis, forums, and blogs. This article examines the effort to find the balance between protecting through restrictions and through cultivating a sense of personal commitment and security ownership among our employees

To try to reduce driving accidents at a dangerous curve in Chicago, the city painted a series of white lines across the road. As drivers approached the sharpest point of the curve, the spacing between the lines progressively decreased, giving the drivers the illusion they were speeding up and nudging them to tap their brakes. The result was a 36 percent drop in crashes, as described by Richard Thaler and Cass Sunstein in the book *Nudge*.

This traffic-control method succeeded in making drivers more aware, improving safety, while keeping the traffic flowing with minimum disruption. I think this example provides a useful metaphor for information security. Some security controls are like stop signs or barriers: we simply block access to technology or data. But if we can shape the behavior of employees rather than blocking them altogether, we'll allow employees, and therefore the company, to move faster.

To use another traffic metaphor, a roundabout at an intersection typically results in more efficient traffic flow than an intersection with stop signs, because drivers don't have to come to a complete halt. The roundabout increases drivers' awareness, but they can proceed without stopping if the way is clear. Statistics have shown roundabouts are often safer than intersections.

Of course, we need to block access in some situations such as with illegal web sites. But there are cases where it's more efficient and productive to make users aware of the risks, yet leave them empowered to make the decisions themselves. For example, it might make sense to warn users visiting certain countries that they may be accessing material that is considered unacceptable. Here's a hypothetical example. A U.S. employee traveling on business might be working in a local office of a country with strict religious guidelines. The employee has a daughter who's in a beauty pageant—so it would be natural to check the pageant web site from time to time. But the images could be offensive in the country,

so it makes sense to warn the employee to exercise caution. At Intel, we've found that when we warn users in this way about potentially hazardous sites, the vast majority heed the warnings and don't access the web sites.

In the case of information security, there's an additional benefit of making controls as streamlined as possible. We all know if controls are too cumbersome or unreasonable, users may simply find ways around them.

We kept this concern in mind when developing a social media strategy at Intel IT. We were well aware of the risks associated with social media, but attempting to stop the use of external social media web sites would have been counterproductive and, in any case, impossible. We realized that if we did not embrace social media and define ways to use it, we would lose the opportunity to shape employee behavior.

As part of our initial investigation into this area, we conducted a social media risk assessment. We found social media does not create new risks, but can increase existing ones. For example, there's always been a risk that information can be sent to inappropriate people outside the organization. However, posting the same information on a blog or forum increases the risk by immediately exposing the information to a much wider audience. We also determined that we could reduce risk by implementing social media tools within the organization.

So we developed a social media strategy that included several key elements. We deployed internal social media capabilities, such as wikis, forums, and blogs. Initially, these were mostly standalone tools, and employees used them mainly to connect socially rather than for core business functions. Since then, our use has evolved to include more enterprise-focused tools, and we have integrated the tools into line-of-business applications to achieve project and business goals. We've also added social media tools tailored for specific business groups, such as a secure collaboration solution used by design teams to simplify real-time sharing of confidential project information across geographically dispersed teams.

As we designed our internal social media capabilities, we also worked with Intel's human-resources groups to develop guidelines for employee participation in external social media sites. Intel then developed an instructional video that was posted externally on a public video-sharing site. The video candidly explains Intel's goals and concerns, as well as providing guidance for employees. It explains that Intel wants to use social media to open communications channels with customers, partners, and influencers and to encourage people to adopt the technology as well as closing the feedback loop. The information also includes guidance about how to create successful content and general usage guidelines such as the need to be transparent, respect confidentiality, distinguish between opinion and fact, and to admit mistakes.

We also use technology to help ensure that employees follow the guidelines. We monitor the Internet for posts containing information that could expose us to risks, and we also monitor internal social media sites to detect exposure of sensitive information and violations of workplace ethics or privacy.

The Security Benefits of Personal Use

In general, people are likely to take better care of their own possessions than someone else's. They feel a stronger connection to their own car than to one provided by their employer. If people are using their own computing device, they may take better precautions against theft or loss. And they may feel the same way if they are storing personal information on a corporate device. At Intel, we allow reasonable personal use of corporate laptops, and therefore many employees store personal as well as corporate information on their laptops. Because of this, they have a personal stake in ensuring the devices don't get lost or stolen.

Many organizations, including Intel, use disk encryption on laptops to protect data in the event the laptop is lost or stolen. Adoption of disk encryption accelerated when states began passing privacy protection laws, and the consequences of data theft increased as a consequence. However with some disk encryption software, the latest data isn't encrypted until the user shuts down the PC or puts it into hibernate mode. If users simply put the PC into standby by closing the lid, the system may contain recently created data that is still unencrypted and vulnerable. If the PC is stolen at that point, the thief still has to penetrate the usual login access controls, but that's much easier than figuring out how to decrypt the data.

When our security group analyzed this data encryption issue, we decided that we needed to be careful about how we addressed it. We wanted to ensure data on laptops was protected, but we didn't want to disrupt the users' experience by forcing them to shut down their laptops more frequently, and then endure the subsequent lengthy reboots. So we adjusted the system settings to initiate encryption whenever the laptop was left unused for a specific length of time. Now, if a laptop is lost or stolen, we can determine the likelihood that it contains unencrypted data, based on the time that elapsed since the employee last used it. While making this change to technical security controls, we also increased our efforts to educate employees about secure behavior.

Insider Threats

It's an unfortunate reality that many intentional threats originate within the organization. Among the 600 organizations participating in the 2011 Cybersecurity Watch Survey, about 20 percent of attacks were attributed to insiders.

The damage can be substantial. One employee working for a manufacturer stole blueprints containing trade secrets worth USD 100 million, and sold them to a Taiwanese competitor in hopes of obtaining a new job with them. Insider attacks also cause additional harm that can be hard to quantify and recoup such as damage to an organization's reputation. Insiders have a significant advantage because they can bypass physical and technical security measures such as firewalls and intrusion detection systems that were designed to prevent unauthorized access.

Yet surveys have also suggested that many insider attacks are opportunistic, rather than highly planned affairs. Many insiders take data after they've already accepted a job offer from a competitor or another company, and steal data to which they already have authorized access. In some cases, misguided employees may simply feel they're entitled to take information related to their job.

It may not be possible to thwart all insider exploits, but we can take action to deter the more opportunistic attacks. Perhaps the biggest step we can take is to try to instill a culture of commitment. But we can also use technology to help against insider attacks.

As part of our security strategy at Intel, we're implementing monitoring technology that tracks users' logins and access attempts. At many companies, IT organizations treat such login data as information that should be closely held and not revealed to users. However, our strategy is to make login information available to users so that they can act as part of the perimeter, helping to spot anomalous access attempts. Let's say an employee's log indicates that he accessed the network from Asia yesterday, when in fact he was in Europe. The security organization might be unaware that anything untoward has occurred. But it's obvious to the employee that someone stole his smart phone or his access information, and he can alert us to the breach.

Providing this login information to users can also help deter insider attacks. If unscrupulous insiders know they're being watched, they're less likely to take advantage. It's like the corner store that invested in a CCTV camera; when you walk up to the counter, you see yourself in the display. Now consider the store on the next corner that lacks a camera. Which one is more likely to be robbed?

Finding the Balance

Whether we like it or not, people are already part of the perimeter. Technical controls alone are no longer able to keep pace with rapidly changing attacks, especially when those attacks are combined with sophisticated social engineering. It's up to us, as security professionals, to recognize that people, policy, and technology are all fundamental components of any security system, and to create strategies that balance these components. Above all, we need to create a sense of personal commitment and security ownership among our employees. If we succeed in this goal, we will empower employees to help protect the enterprise by making better security decisions both within and outside the workplace.

==========

This article is based on material found in the book "Managing Risk and Information Security" by Malcolm Harkins. Visit the Intel Press web site to learn more about this:
http://noggin.intel.com/intelpress/categories/books/protect-enable

Also see our Recommended Reading List for similar topics:
www.intel.com/technology/rr

About the Author

Malcolm Harkins is vice president of the Information Technology Group, and Chief Information Security Officer (CISO) and general manager of Information Risk and Security. The group is responsible for managing the risk, controls, privacy, security, and other related compliance activities for all of Intel[1]s information assets.

Before becoming Intel's first CISO, Harkins held roles in Finance, Procurement and Operations. He has managed IT benchmarking efforts and Sarbanes Oxley systems compliance efforts. Before moving into IT, Harkins acted as the profit and loss manager for the Flash Product Group at Intel; was the general manager of Enterprise Capabilities, responsible for the delivery and support of Intel's Finance and HR systems; and worked in an Intel business venture focusing on e-commerce hosting.

Harkins previously taught at the CIO institute at the UCLA Anderson School of Business and was an adjunct faculty member at Susquehanna University in 2009. In 2010, he received the excellence in the field of security award at the RSA conference. He was also recently recognized by Computerworld magazine as one of the top 100 Information Technology Leaders for 2012.

Harkins received his bachelor's degree in economics from the University of California at Irvine and an MBA in finance and accounting from the University of California at Davis.

==========