Cisco on Cisco Best Practice

Security Practices for Online Collaboration and Social Media

January 2012

Contents

Introduction

Online tools for desktop sharing, audio and video collaboration, and enterprise social software play an increasingly important role in corporate business. The industry is also seeing a trend toward “IT consumerization,” where employees and other users experience new technologies before they are supported by enterprises. The first impact of this trend is producing more employee requests to access their personal social media accounts from their work computers as a way to manage both work and life responsibilities. The even bigger impact is that employees want to use these types of collaboration tools for enterprise business purposes.

The goals behind collaboration and social media tools are clearly beneficial to business—better information sharing, more efficient decision-making, and enhanced business relationships, among others. And trends are clearly indicating that collaboration will become a fundamental way of conducting many types of business activities in the near future.

However, online collaboration tools—and external social sharing tools in particular—present security risks to the operation of enterprise networks and computing systems, as well as to the confidentiality of intellectual property and business information. But an organization that tries to completely ban external social media will likely find that employees may ignore the rules and use those tools anyway, by circumventing corporate processes. And this unauthorized, unmonitored, and uncontrolled use can increase the IT and business risks.

Given these challenges, it may be tempting to simply block the use of collaboration and social networking tools. Yet doing so will place a business at significant disadvantages in a world that is increasingly connected by shared information.

Through continual learning and process changes, Cisco IT is moving toward the right balance between the desires of employees to share and the business requirements of maintaining IT security, data, privacy, and asset protection.

The Challenges of Securing Online Collaboration and Social Sharing

Specific challenges faced with social sharing and online collaboration include the following:

Social engineering and intelligence gathering. Social engineering is an effective online technique for someone who has malicious intent. For example, a person could create a deceptive Facebook or LinkedIn account and start “friending” people within a company in order to gain trust and familiarity. After a time, this person can ask for—and

receive—confidential information from unwitting employees. It is just a matter of deceiving the first few employees and gaining their trust. When others see their fellow employees as contacts, they are more inclined to accept an invitation from the perpetrator, which furthers the intelligence gathering. The whole idea behind this technique is exploiting the trust that employees place in each other.

Collaboration and social sharing tools can also give a competitor, a hacker, or a criminal an easy way to gather valuable information. All it takes is time and patience to find the information that is casually disclosed on social networking sites. Although separately these small bits of information may not be useful, when assembled together, they can provide big and profitable insights. This data can then be used to hack into computing and network systems, expose or steal sensitive data, tamper with financial accounts, or disrupt a company's operations.

Network attacks originating as social messages. Viruses, worms, phishing schemes, and other forms of malware can be spread easily through links in text messages to a mobile device, social media update messages (e.g., tweets), and advertisements on social sites. For example, emails that appear to contain an invitation for connecting on a social networking site such as Facebook or LinkedIn may actually contain malware or a Trojan Horse.

Sharing confidential and proprietary information too freely. The traditional view of tightly restricting information sharing is changing in the face of expectations for openness in the new social world. When an employee can easily make—and share information with—business connections both within and outside the company, the opportunities for improper sharing increase significantly.

Much of the risk for improper sharing comes from lack of user training about collaboration security concerns and lack of guidelines for appropriately posting or disclosing information online. Users may incorrectly believe that small pieces of information posted on a social site won't do harm, or that information they share in a personal social account won't cause a business security threat. Users may also feel it is okay to trust and respond to online information requests from people who identify themselves as "friends" or fellow employees, even if those users might be more cautious about disclosing that information in another setting.

Limited security in social sharing tools. In most cases, the security settings in a social sharing tool—or in employee's social accounts—cannot be controlled by the enterprise. And some tools, especially open-source social software, may not have important security capabilities. To compensate, additional security measures may need to be implemented on the enterprise's collaboration platforms and network.

New types of security measures, policies, and practices. The IT security technologies, policies, and processes an organization already has in place will continue to play an important role as business activity becomes more collaborative. But it may be necessary to create additional policies and practices to protect confidential data and systems from the threats in social sharing.

These policies and practices should be specific to a company's operations and risk factors. For example, companies in highly regulated industries may not be able to allow the open posting and collaboration that occurs on social sharing sites, especially those external to the company.

Once these policies are in place, it is important to explain and enforce them with employees. In the 2010 Cisco Connected Technology study, workers around the world indicated they are more likely to break an IT policy if they believe there are no repercussions for doing so. In addition, the study found that when IT policies are not developed with a relevant rationale, they are likely to be met with employee apathy and selective compliance.

Preparing for "borderless" collaboration. Extending collaboration and social sharing externally can produce new benefits and relationships with customers, suppliers, and business partners. However, borderless collaboration also brings new security questions, such as: What level of access do you give and to whom? How do you protect each other's confidential information?

How Cisco is Addressing Collaboration Security

In most cases, Cisco allows employees to use collaboration tools and access social networking sites while at work and to conduct business. This corporate openness is balanced through the company's policies, guidelines, and training for users as well as security measures in the Cisco collaboration technology and network.

Cisco Corporate Policies and Guidelines

Cisco presents its social networking policies and guidelines in several documents and online resources that can be found easily by employees on the company's intranet.

The Cisco Code of Business Conduct (COBC). The Cisco COBC document is a centerpiece of the company's expectations for the business activity of employees, including all forms of online communication. The code describes how to protect Cisco's intellectual property information assets, as well as the confidential information of customers and partners that is maintained by the company.

As a publicly traded company, Cisco must also comply with strict regulations about financial reporting. The Cisco COBC presents the special policies that govern disclosure of financial and investor information.

One security concern covered by the Cisco COBC is employees who share information too freely inside the company, with other Cisco employees or contractors. A COBC requirement is that employees share confidential and proprietary data only with co-workers who have a legitimate business need for that information.

To emphasize the code's importance, Cisco requires employees to sign a COBC acknowledgment statement every year.

Cisco Social Media Handbook. A core document containing social collaboration policies and guidelines is the Cisco Social Media Handbook. Cisco employees, vendors, and contractors are expected to follow these guidelines when posting any type of content to blogs, wikis, discussion forums, and social networks. The guidelines apply to all social sites, whether internal to Cisco, hosted on Cisco.com, or for public sites.

Content in the Handbook is developed and maintained by a team that includes representatives from Cisco's corporate communications, marketing, legal, information security, and employee relations departments as well as the company's chief privacy officer. The team meets regularly, knowing that social media guidelines must be updated frequently to keep pace with changes in social technologies, customs, and best practices. Cisco also provides sufficient training to employees, especially those who may come across and use these social tools for day-to-day business.

Cisco corporate information security policies. Cisco expects every employee to comply with policies established by the company's information security (InfoSec) department that cover topics such as:

- Data classification and protection
- Password protection on user accounts and devices
- Remote access by PCs and mobile devices to the Cisco network
- Appropriate use of computing devices and networks

Cisco issues a laptop PC to each employee for business use and allows employees to access the Cisco network from their own, approved smartphones and tablet computers. All of these devices must comply with Cisco InfoSec requirements for security features and updates. Additionally, employees must acknowledge that Cisco has the right at any time to inspect all messages, files, data, software, or other information stored on these devices or transmitted over any portion of the Cisco network.

As it pertains to collaboration, use of cloud services and direct file sharing are additional topics to consider for an information security policy. However, because of the security risks in cloud services and direct file sharing, a Cisco security team monitors the activity and ensures that the involved employees are following Cisco's acceptable use policies. Employee communication and training about the security risks involved are also very important aspects of enforcing this policy.

User Training and Information Resources

Cisco operates under the principle that employees can be trusted to do the right thing and make the right decisions if they have been well-trained about collaboration security measures. Of course, this training won't eliminate all security risks, but it can significantly reduce the number of threat incidents and their impact.

Cisco offers employees an in-depth security education program, with training on collaboration topics such as recognizing social engineering tactics and appropriately tagging content to prevent inappropriate sharing. Cisco also teaches employees about the importance of protecting company data on their business and personal social media accounts. Particular guidelines include:

- Be careful not to inadvertently disclose proprietary information in the spirit of being "helpful" to online connections.
- Avoid being too casual about trusting so-called "friends of friends" because these social accounts may be fake. Connecting to that "friend" can create an opening for a social engineering attempt to gather knowledge or to launch a network attack through the employee's PC.

Cisco uses both Cisco TelePresence and Cisco WebEx collaboration tools to deliver the training workshops as well as internal social media certification programs.

In addition, an internal global social media community provides guidelines, documents, short video tips, FAQs, and a discussion forum where employees can seek advice about social web issues.

Security Measures in Collaboration and Networking Technology

The best strategy for reducing and mitigating the threats that can come from online collaboration and sharing is to follow defense-in-depth security practices. These practices control access to sensitive systems and websites, then define what users can see and do when they are granted access.

User identity, authentication, and authorization (AAA) technologies. Review AAA configurations in light of the greater sharing involved with collaboration and for allowing access to internal collaboration tools by contractors, suppliers, business partners, and customers. Cisco is implementing an advanced identity management framework that will use the Cisco Identity Services Engine for granular user identity and access control. This framework is important for an increasingly "borderless" world, where users may present more than one access persona through a combination of devices, locations, and use of systems, applications, and data. Cisco IT is deploying the Identity Service Engine to provide a dynamic, context-aware policy framework that will increase protection of internal resources and sensitive information.

Security design for the collaboration platform. How the collaboration platform is implemented within the network and system architecture is an important factor for security. Cisco uses its own Cisco Quad™ platform for the company's internal collaboration and social sharing site, called the Integrated Workforce Experience (IWE).

Table 1 shows the security design principles followed by Cisco IT for its implementation of the Cisco Quad platform.

A. Cisco IT Security Design for Cisco Quad Deployment

Security Design Principle	Deployment Decisions
Maintain Cisco IT's existing, tiered application architecture	Create a separate tier for the public-facing Cisco web service Place all Quad services for applications within a separate, protected tier Store all data on internal servers
Control all traffic into the application tier with specific security rules	Allow only known traffic; use firewalls to protect the Quad platform from unauthorized traffic; use intrusion prevention systems to monitor access
Control traffic from the Quad platform into corporate systems	Allow only application traffic to reach corporate systems, and only via approved network services
Cisco Quad applications can access the Internet, but must try to identify and remove malicious content from untrusted data received from the Internet	Use the industry-developed AntiSamy API to prevent malicious code that comes through an RSS feed or comment on a blog post from persisting on the server Use the Cisco IronPort™ Web Security Appliance as an Internet gateway

In addition to securing the collaboration platform, it is also important to secure the content and tools that run on that platform. For example, application portlets are an appealing way to tailor the content and features of internal collaboration and social sharing platforms to specific departments and user communities. However, these add-ons may become a point of security vulnerability, especially when they access confidential information (e.g., financial data) or sensitive functions (e.g., purchasing). Create procedures to verify the security of portlets and applications—especially those developed and maintained by third parties—that integrate with your enterprise social software.

To prevent unintended content disclosure by inexperienced users, the Cisco Quad platform supports role-based and rule-based access restrictions to help employees appropriately define who can see what. Together, these restrictions support the concept of granting only the level and type of content access that is necessary for a particular employee's work.

Built-in security features with collaboration products. Take advantage of the built-in security features in collaboration technologies such as Cisco TelePresence, video calls, and Cisco WebEx. For example, Cisco WebEx offers many features to control user accounts, meeting participation, client authentication, and content encryption.

These features help prevent unauthorized access to the meeting sessions and data capture as the meeting traffic is sent over the Internet.

Network security solutions. Core network security technologies play a very important role in protecting against and mitigating collaboration security risks. For example, the Cisco IronPort Web Security Appliance is a secure web gateway that helps to enforce acceptable use policies, protect against malware, improve data security, and provide visibility and control into browser-based applications. The appliance also blocks a variety of potential security threats by validating the source site before the code can be downloaded. The Cisco ScanSafe solution complements an on-premises solution based on Cisco IronPort to provide endpoint security through a cloud model.

The Cisco Intrusion Prevention System (IPS) protects against sophisticated network attacks including directed attacks, worms, botnets, malware, and application abuse. Cisco IPS technology also recognizes and blocks the spread of a Trojan Horse from an employee's PC to corporate computing systems over the enterprise network. This response reduces the potential for loss from application disruptions, data theft, or website defacement.

Cisco IT performs regular, extensive audits of its security technology deployments to make sure they are up-to-date with the latest threats and best practices.

How to Get Started with Collaboration Security

The following steps can help establish appropriate security policies, technologies, and processes related to collaboration and social media security:

- Create a business plan for collaboration and social networking solutions, starting with the business need.
- Craft clear security governance mechanisms for collaboration.
- Create policies on information confidentiality and expectations for employee activity when interacting on collaboration sites.
- Define policies on network security measures such as remote access by mobile devices, level of password protection, and use of direct file sharing.
- Identify regulatory and compliance requirements that might restrict use of or information disclosure on social media.
- Create training resources for all users.

For More Information

Collaboration Security Resources

- The Cisco Social Media Handbook is available for download at: www.scribd.com/doc/33461366/Cisco-Social-Media-Policy-Guidelines-and-FAQs
- The Cisco Code of Business Conduct document is available for download at: http://investor.cisco.com/documentdisplay.cfm?DocumentID=3263
- Information and resources about Cisco policies and practices for online privacy are available in the Cisco Privacy and Compliance portal: www.cisco.com/go/privacycompliance
- A step-by-step guide for creating a security education program is available at: www.cisco.com/go/securityeducation
- To read the Cisco Connected Technology World Report, visit: www.cisco.com/en/US/netsol/ns1120/index.html

- Guidelines for protecting WebEx meeting sessions are presented in the Cisco WebEx Web Conferencing Security White paper: www.cisco.com/en/US/prod/collateral/ps10352/ps10362/ps10409/WebEx_Solutions_Security_Overview.pdf

Cisco Products and Services

- To learn more about Cisco collaboration solutions, visit: www.cisco.com/go/collaboration
- For information about Cisco security products, visit: www.cisco.com/go/security
- Cisco also offers professional consulting services for collaboration security: www.cisco.com/go/collaborationservices

To read additional Cisco IT best practices and case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**