

Cyber security in a borderless world

Three prevalent technologies – social media, mobile devices, and cloud computing – substantially expand the attack surface of your enterprise.

Rapid adoption of social media, mobile devices, and cloud computing has expanded the traditional borders of the enterprise – creating multiple new entry points for cyber attacks. However, security capabilities in many companies have not yet caught up. Here are some specific steps CIOs can take.

This is the third article in a three-part series on cyber security. The first article discusses ways to talk to senior executives about the realities of the evolving cyber security landscape, while the second asks you to consider whether your IT security approach is up to the task of addressing today's threats.

Anti-social Media?

Social business is built on platforms that enable stakeholders to communicate, collaborate, and conduct business around shared passions, pains, or common traits. Businesses large and small have the ability to monitor, participate in, and even shape their discussions. But social media sites and collaboration tools can open an enterprise to countless new avenues of attack. A Deloitte Touche Tohmatsu Limited survey¹ of technology, media, and telecommunications companies showed that more than 80 percent of security IT professionals interviewed consider as threats "exploitation of vulnerabilities in Web 2.0 technologies" such as social networking sites, blogs, wikis, and the like.

Social media provides more avenues from which an attack may be launched as well as more surface area to protect against such attacks. The external threat patterns are now familiar. Attackers use social media to identify, profile, and compile personal data on targets. Data aggregation from multiple sites can lead to compromised passwords, data leakage, and security incidents. Criminals use available data to build profiles of executives for identity theft or actual attacks.

Meanwhile, internal threats – for example, employees who leak intellectual property, inadvertently violate privacy laws, or distribute confidential information to the public at large – pose another insidious source of danger.

Whether the goal is to steal intellectual property, commit fraud, damage the company's reputation, or otherwise cause harm, determined criminals can usually find a way. Moreover, traditional techniques like phishing can be easily applied in the realm of social media since they don't require detailed knowledge of email systems or IT infrastructure. While you cannot stem the tide of information flowing across the borders of the organization, you can mitigate the risks.

Three steps can help you avoid threats from social media:

- Define the threat. Understand the features and dangers of specific social media sites and collaboration tools. Identify how peoples' activities in these systems – both at work and at home – can expose private information or create other risks.
- Create boundaries. Establish policies governing the use of social media and collaboration tools. For starters, focus on preventing data loss and reducing employees' "digital exhaust." Use available technologies such as web filtering and data loss prevention software to shore up defenses.
- Educate your workforce. Make people aware of the risks in social media, the policies governing their use, and how they can use social media safely. When incidents occur to other companies, share those examples as lessons for your employees.

Mobile devices create new points of entry

As business people adopt smartphones and tablets for their work – and other stakeholders adopt them to interact with businesses – organizations are recognizing the opportunities and potential value of mobile applications. But, benefits aside, smartphones, laptops, notebooks, and tablets present relatively easy, low-risk points of entry to your systems. Attackers can remotely monitor them for passwords, account numbers, personal data, and proprietary information. Stored passwords on lost mobile devices can provide attackers with immediate access to your systems. Although mobile devices can be outfitted with various levels of protection, poorly planned approaches promote ad hoc efforts and force needless tradeoffs between ease of use and security.

Device management software and tools are still maturing, making it difficult at times to efficiently control distribution of applications and to monitor and control devices. Additionally, differing versions of hardware and software can make it difficult to ensure the right software is running – and up to date – on each device.

There are also human issues, such as executives who demand exemptions from security policies for their personal devices or users who permit others to access their devices. The issue of control is exacerbated when employees are allowed to use their own personal devices to access corporate infrastructure. In general, people tend to exercise less care for security with mobile devices than they do with desktop computers.

The following precautions can help you cope with cyber threats posed by mobile devices:

- Know what's at risk. Start by understanding how devices are being used by different segments of users. Determine what, if any, sensitive data is stored on mobile devices and what access to corporate infrastructure those devices provide. Then develop a risk-based approach to managing devices that takes into account the organization's culture and willingness to allow devices to be managed.

Lock it down. Configure mobile devices with encryption and a password-based login to minimize their chances of being scanned, sniffed, or tampered with. Establish and implement conditions under which a device can – or cannot – connect to corporate infrastructure.

Understand geographic risks. Pay particular attention to overseas travel, and develop a geography-specific, policy level approach to deal with risks in various countries. For example, the policy may prohibit Wi-Fi connections in one country or may require users to remove applications containing sensitive data when traveling to another.

- Employ policies. Establish corporate-wide policies specifically for mobile devices. Publish application whitelists – telling users what software is considered safe – to prevent malicious software from running on a device. Also, issue guidance regarding security capabilities and procedures so employees can make smarter purchases and take the right precautions.
- Make it wipeable. Ensure that all phones used for corporate business can be wiped clean in case of loss or tampering. Some devices allow users to remotely delete all data, or will destroy data after a certain number of failed login attempts. Several software companies provide installable applications with the same functionality. Also ensure all devices are backed up regularly to avoid losing important data.

Seeing into the cloud

Cloud computing offers flexible new ways to manage IT costs, scale operations, and streamline processes. It also presents new security and privacy threats that vary with the type of cloud, architecture, and purpose. Risks will vary, for example, across infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) offerings. But one fact is constant: When you contract for cloud services, you hand over critical operations and data to an entity you do not directly control.

While reputable cloud providers have strong incentives to manage security wisely, and often have made a more substantial investment in security than the companies they serve, you cannot simply assume your provider is doing all it can. Every cloud service provider is different. Some limit what customers can inspect, potentially placing the data center out of bounds. This can spell trouble in a multi-tenant, virtualized world, especially in foreign locations. In any environment, you must know where the cloud components – and your data – will be housed and who is responsible for which functions and risks.

Most enterprises understand the conventions of the countries in which they operate. But cloud service providers may house your data in different jurisdictions, or transport your data among them, thus potentially introducing different risks and regulatory obligations. If your organization needs to produce an audit trail or specific tax or legal data, be sure the required capabilities are in place.

To manage cyber threats and risks associated with public cloud computing:

- Categorize your information and operations by risk. You may be comfortable sharing some aspects of your operations with cloud providers, while maintaining full control over others, based on an assessment of all manner of risks (regulatory, risk, business continuity risk, integrity risk, and more).
- Establish standards. Define your own standards and then, to the extent possible, apply them to service providers and business partners. Remember, you can transfer some risks such as the risk of hardware failure – but there are likely many other risks – regulatory and reputational risk, to name two – that you won't want to transfer.
- Trust but verify. Due diligence when selecting service providers is a must – as is addressing each party's rights and responsibilities within the contract. Then, monitor the situation regularly to ensure the standard is being effectively applied, and whether any changes have been made in your providers' security practices.

The globally-connected, highly-mobile, always-on technology culture is tearing down the traditional boundaries of every organization. Organizations are increasingly managing more distributed environments where key processing and data are managed by infrastructures outside of their direct control. Clearly, traditional wall-and-fortress security measures have been rendered less effective against many security risks. In this fast-moving environment, detecting and monitoring what happens beyond the bounds of the fortress becomes an essential security capability. For social media and mobile devices, a mix of user education and measures to protect devices can heighten security.

For cloud computing, the due diligence applicable to any important outsourcing vendor would be called for, as would carefully constructed contracts and periodic contract risk and compliance analysis. The essential point is that, as your employees and your company adopt new ways of working, security needs increasing focus, creativity, and agility to keep up.

May 23, 2012, Irfan Saif and George Westerman, MIT Center for Security & Privacy Solutions

Contact

James Nunn-Price
+44 20 7303 8708
jnunnprice@deloitte.co.uk

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.co.uk/about for a detailed description of the legal structure of DTTL and its member firms.

Deloitte LLP is the United Kingdom member firm of DTTL.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication. Deloitte LLP would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte LLP accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

© 2013 Deloitte LLP. All rights reserved.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom. Tel: +44 (0) 20 7936 3000 Fax: +44 (0) 20 7583 1198.

Designed and produced by The Creative Studio at Deloitte, London. 24346A