Preparing for the Top IT Security Threats of 2013

Wisegate CSO members share strategies for combating next year’s biggest IT security threats
Introduction

To stay ahead of IT security threats, it’s helpful to learn what other CSOs are doing and have done, and to replicate their successes and avoid their pitfalls. Wisegate recently organized a community discussion among CSO members across multiple industries to talk about the top anticipated security threats of 2013 and how to prepare for them.

The general consensus among CSOs is that specific threats—like the latest virus in the wild or DDoS attacks that groups like Anonymous are threatening to launch—are not the most urgent security concerns to address. Rather it’s broader areas such as mobile computing, BYOD (bring your own device), cloud computing, and data protection that will need their heightened attention in 2013. Within these areas many CSOs are planning to devote more resources, develop policies and procedures, evaluate and implement solutions, and provide awareness training.

As one CSO points out, the nature of the present-day threats aren’t necessarily new, but it’s the attack vectors and manifestations that change over time. For example, data loss is a perpetual concern—as a threat to business privacy and security—just as it has been for decades. But the fact that workers increasingly use their own smart phones to access corporate data puts a new spin on the old problem of potential data loss. It is with this perspective that Wisegate CSO members discussed:

» What are the top IT security threats in 2013?
» What are the potential impacts of these threats?
» What proactive strategies help companies stay ahead of the threats?

The Top IT Security Threats of 2013

Broadly speaking, the main threats that CSOs see today have one underlying root cause: the universe of available IT resources—devices, applications and services—is no longer fully under the control of an official IT department. Business units and even individual end users are deploying their own resources, such as smart phones, SaaS applications and cloud-based data storage that may not meet corporate security standards but still have access to the company network or data. This introduces a wide range of IT security threats that are completely unintentional but no less real.

CSOs cite the following concerns as some of the biggest security threats to their respective organizations.
BYOD – Bring Your Own Device

Wisegate CSO members are in complete agreement: allowing workers to use their own mobile devices (including smart phones, tablets, and notebook computers) presents a serious threat to network and data security. While CSOs believe that BYOD can help workers be more productive in their jobs, they are concerned that workers don’t take proper security precautions, and there is a lack of controls, which are needed to protect company data. For example, one CSO cited a case where a home-based worker allows her children to play Internet games on the same tablet computer she uses to access her work files. These situations puts the organization in the difficult position as the IT becomes responsible for setting policies and deploying technologies that will protect the business without restricting what the employees can do with their personally owned device.

CSOs express specific BYOD concerns about:

- The theft, loss or leakage of company data
- Proper storage and transmittal of company data (e.g., storage in the cloud or transmittal via Dropbox)
- The limitations of managing devices, and how far the organization can or should go toward locking-down devices
- Malware and spyware aimed at mobile devices
- How (or even whether) to support a growing number of devices that use a variety of operating systems, applications, firmware and mobile carriers

Social Media

Many organizations are seeing a blending of work and personal identities as employees use tools like Twitter, LinkedIn or Facebook when communicating with customers, partners and friends. Members note that there is a need for enforceable policies and procedures as well as awareness training to help control the type of information workers share on a personal level when it might be connected with work assets. For example, a worker might mention a work project, discuss business travel, or identify the name of his or her manager using social media. Such details can be used for spear phishing attacks and may potentially reveal confidential company information.
The General “Consumerization” of IT

Beyond BYOD, and beyond the use of social media, there is a broader issue with the consumerization of IT. Many employees are now using technologies and solutions that were originally developed for consumers to accomplish work objectives. One CSO cites the example in which the company provides an FTP server for the controlled transfer of data, but workers eschew it in favor of the user-friendly tool Dropbox. Similarly, employees store data in the cloud because consumer-oriented storage services are readily available and easy to use. Unfortunately, there are aspects of these tool sets that are wide open, completely lacking security controls. This reality is contrary to normal risk and control procedures where applications, data and tools are supposed to be highly controlled.

One Wisegate CSO member says he is seeing more Apple MacBook computers within his environment. Traditionally Apple computers haven’t been in the enterprise, but now his team is looking at the same issues they faced with Windows-based PCs: imaging, asset management, malware and spyware protection, etc.

Another aspect of the consumerization of IT is the ease in which users and business units can create their own unofficial company-related website or hosted cloud applications by simply contacting GoDaddy or some other ISP to claim a domain name and set up a website that is outside the company purview and control. In addition, the use of consumer-grade products and services is causing the network perimeter to disappear as organizations allow more unmanaged mobile devices to access more data. This creates potentially serious data and compliance issues.

IT Security Awareness

All Wisegate CSO members expressed concerns about the challenges they face in making employees aware of IT security practices. Getting people to understand what corporate information is, and why it must stay within secure corporate resources, can be difficult. It takes significant effort to make sure employees don’t put corporate information where they shouldn’t, such as on a consumer-oriented service like Dropbox. Ultimately people want to take advantage of new technologies to be efficient and effective as they can be—even if the technologies they choose lack appropriate security controls. For this reason, IT security awareness will always be a significant challenge.

One CSO shared his experience of bringing ex-hacker Kevin Mitnick to speak to his co-workers. It was a real eye-opener to hear how easy it is to gain workers’ confidence and use that confidence to gain access to corporate resources. Companies see similar situations with phishing and spear-phishing attacks that trick workers into revealing information or performing a harmful action.
Another set of CSOs expressed the need to gain a level of awareness at the executive and Board of Directors level. Good security practices have to start at the top and be baked into business decisions at the outset.

On a higher level, other CSOs are concerned about the potential impact of the Cyber Security Act. Though Congress did not pass this legislation in 2012, lawmakers might enact the law in 2013. With its mandate for board awareness of both cyber security and information security risks, this act has the potential to create a tremendous ripple effect throughout every industry. CSOs believe it’s important to preemptively prepare so that if the law gets passed, a plan and strategy is already in place.

Cloud Computing
As more services are moved into the cloud—whether it’s hosting an infrastructure as a service, or taking advantage of software as a service—CSOs note the importance of making employees aware of the issues that come along with these services. This includes issues such as data compromise and loss, and uptime reliability. One CSO’s company had the unfortunate experience of becoming “collateral damage” when another company that shared the same cloud infrastructure was targeted for a DDoS attack. Companies often turn to the cloud before making a thorough assessment of the risks.

Data Protection
At the heart of every IT security program is company data that must be protected. The issues mentioned above—BYOD, consumerization of IT, social media, cloud computing, security awareness—all have a big impact on data protection. Wisegate CSO members worry that corporate data is ending up in places where it shouldn’t be, or where it isn’t secure: on workers’ smart phones, on consumer service platforms, and in cloud applications that are unknown to the IT department. Organizations need to implement controls and awareness programs to assure that employees do not put sensitive information where it is not adequately protected.

Many CSOs expressed concern about long-term distribution of data as their organizations begin to use Big Data techniques. With the data being widely distributed across hundreds of servers, there is the potential to forget that the data is “out there”—yet it is. One CSO believes that five years down the line we’ll be talking about how sensitive data was recently discovered in an unsecure library.
Another big issue is losing track of data, specifically where it is stored and the controls around it. For example, most organizations have controls around their storage areas, but then one day the controls are not in effect. Why? Because there was some change to the system(s) and access to the resource is now inadvertently wide open. Additionally, employees will store data in an area that’s convenient to them or convenient to people they want to share the data with. Most of the time organizations do not know this has happened until an outside party tells them that their data was compromised. Unfortunately, it’s becoming almost impossible to track all the places where corporate data has been stored and manage the controls that may or may not be there. (While we don’t mean to pick on tools such as Dropbox, CSOs dread this type of application because it has no controls around it.)

Proactive Strategies: What Wisegate CSO Members are Doing to Stay Ahead of IT Security Threats

The first step to overcoming any security challenge is identifying what the problem is; the second step is figuring out how to address it. Preferring to be proactive rather than reactive, Wisegate CSO members are always devising new strategies to stay a step ahead of the biggest security threats.

Awareness… More Awareness and Teaming

Sometime the best approach to reducing security and control risks—which can include spear-phishing attacks via social media or creating cloud-based applications without IT support—is to get out in front of the issues with employee awareness and education programs. All of the CSOs are actively educating employees and business unit leaders about the most prevalent security threats and risks they pose to the organization.

The consumerization of IT is causing unique problems. In many cases, employees just don’t see the risk associated with their favorite devices. Intuitively they understand why a company-owned laptop might need to be encrypted, but they have difficulty understanding why they can’t have Angry Birds and a PCI-compliant application on the same iPad.

Everyone needs to recognize that technology is not the only solution. As one CSO points out, constantly trying to fix people problems with technology is just throwing money down the drain. Technology is important, but at the end of the day employees must be more aware. Moreover, training and awareness need to be more than just a compliance sheet tick mark. Too often, companies equate “training” with the desired “behavioral change,”
and they aren’t necessarily the same. Employees need to understand how their actions help
or harm their own security posture before they are likely to adopt more secure behaviors.

In particular, workers are being exploited through social engineering and spear-phishing
attacks. To counter this menace, employees must understand that not everything coming
through email, even though it looks legitimate, actually is legitimate. Wisegate CSO
members say they emphasize employee training in this area to reduce the likelihood of
exploitation by unseen attackers.

One CSO is looking for ways to quantify the threats as a metric; for example, he wants
workers and company leaders to be aware of how many times a virus or malware has been
blocked before it could reach a worker’s computer to do harm. Rather than hide security in
the background, he believes workers should know how often automated techniques are
called upon to mitigate the threats. His intention is to lead people to change their behaviors
that may be opening the door to the threats; for example, using a company email account
to receive personal email messages, or clicking on suspicious email without thinking about
the ramifications.

One CSO stresses the value of engaging with the business units to determine how
technology is integrating with their business processes. From this joint view, it can be better
determined where threats are coming from, the impact they have on the business
processes, or even whether changing or enhancing business processes can reduce
exposure to security issues. The goal is to make sure that information security is baked into
business processes rather than trying to bolt it on later.

**IT Department as the First Adopter**

Many Wisegate CSO members are strategically asking the IT Department (along with
support from infosec professionals) to be the “first adopter” of the technologies that are
likely to come into the company environment. This includes popular consumer technologies
such as handheld devices and applications. By trying new technologies before end users
bring them into the work environment, IT can better understand potential security threats as
well as support requirements. More importantly with a first adopter approach, the IT group
becomes the enablers of business units and their staff rather than being the gatekeepers—
or worse, the preventers.

This kind of proactive approach helps organizations deal with issues before they become
actual threats and allows security to be built into the technology adoption process. Ideally,
the IT Department can perform the security and risk assessments and data classifications
as needed to ultimately put the appropriate security measures in place—all before a user asks for such a tool.

Of course, this approach requires senior management sponsorship. Without a proactive strategy, the secure adoption of enabling technologies—from cloud applications to social media, and smart phones to tablets—could be impeded.

**Network Segmentation**

A number of CSO’s say they are addressing some common security issues through network segmentation. For example, one organization has all of its main applications on a Citrix environment where it minimizes the amount of threat or impact that local workstations can have. In this environment, the workstation can be one of the least significant components of the network. This company has two ISP’s and they use a firewall to split the traffic so that one ISP circuit is for business traffic only, and the other is for everything else. Instead of trying to prevent workers from doing certain things, the organization is enabling them to do it in a manner that doesn’t impact business operations. If an end device gets a virus or is otherwise compromised, the company can easily reimage it without losing anything.

With such an approach, data is in one area, the applications are in another, and the desktops are in yet another area. The company compartmentalizes everything and channels personal identities away from work identities without impacting the workers or the work.

**Network Visibility**

Some Wisegate CSO members address their security issues by analyzing what is really happening on their network. Using tools for increased visibility, they can determine what normal network traffic patterns look like and be more prepared to identify abnormal patterns that might indicate a security incident. They’ve deployed the increased visibility along with network segmentation in order to normalize traffic between different classes of servers like database, file and mail servers.

**In Closing…**

IT operations and infosec professionals have their work cut out for them in the year ahead. Though security threat vectors are changing, the underlying principles of how to address them are not. It’s important to get out in front of potential threats and involve everyone in the organization. Increasing employee security awareness and convincing workers to adopt
more prudent behaviors will go a long way in complementing the technology-based solutions that organizations deploy to protect their network and information assets.

A more in-depth discussion on information security threats and strategies continues online at www.wisegateit.com.

Wisegate is an IT expert community and information service that provides senior-level IT professionals with high quality research and intelligence from the best source available—the collective knowledge of IT leaders from across the industry.

Through live roundtable discussions, detailed product reviews, online Q&A and polls, and timely research reports, Wisegate offers a practical and unbiased information source built on the real-world experience of veteran IT professionals. No analyst theories or vendor bias to cloud the information, just clear and straightforward insight from experienced IT leaders.

Would you like to join us? Go to wisegateit.com/request-invite/ to learn more and to submit your request for membership.