

HELLO. I'D LIKE TO THANK EVERYONE FOR COMING TODAY.

Today I'll be discussing the threat that insiders can pose to corporations.

[Slide 1]

As security professionals, our focus has traditionally been on the external threat. We've spent a great deal of time and money bolstering our perimeter security to thwart the Internet "hacker". Most organizations have done an admirable job pursuing these goals, while often ignoring the threat that may be posed by those who already have access to internal networks.

In other words, we've focused on the hard candy shell, and not the soft gooey core. Nevertheless, technology today is causing the perimeter to erode.

Insiders include anyone authorized to access internal systems. This includes employees, but it also includes our business partners. We share information and collaborate with suppliers and dealers and customers. Business leaders see new uses of information technology as ways to increase productivity, reduce costs and innovate. Think of technologies such as virtualization, social media, mobile devices and cloud computing, as some examples of where insiders are introducing new risks into the environment. So, we have a more diverse set of insiders, doing more than ever before. The advent of new technologies and the desire to cut costs has made our job of managing the insider risk more difficult.

The insider threat is not new. We've traditionally considered insiders to be employees, but as I've said, that's not always the case. Today, it is routine for corporations to provide Internet access, via VPNs and other means, to suppliers and contractors so they can develop code or maintain internal systems. Firewalls, system logs and Intrusion Detection Systems aren't up to the task of monitoring and managing the insider activity that we face today.

[Slide 2]

Insider threats can be seen as either intentional attacks, security avoidance, mistakes or just due to ignorance of the law.

Intentional attempts to steal data or harm systems aren't usually the most common, but we'll talk in a bit about how these may be on the rise, due to external factors, such as the economy. These threats include direct theft, eavesdropping, accessing unauthorized files or abuse of systems.

You may not think security avoidance is common, and hopefully it is less common now that it was a decade ago. Back then, security policies were strict and since security was less mature, policies often failed to take into account business realities. Even today, if security policies and processes are seen as too expensive or in the

way of “business innovation” or efficiency, then employees may take it upon themselves to skirt security rules. In some cases, managers may even encourage this. This threat is best addressed by engaging with the business, making sure that security policies are aligned with business objectives and applying risk management techniques to find innovative ways to architect security solutions that are both flexible and secure.

The third category is mistakes, misconfigurations and oversights. These are not uncommon, but through security in depth and with good processes these can be minimized. It’s not JUST misconfigurations, another example would be losing valuable data, because we didn’t think that employees might take data home on a USB drive.

And finally, insiders don’t always know the rules. This emphasizes the need for better security education, as well as concise security policies that are easy to find and understand.

[Slide 3]

The recent economic downturn has raised concerns that the insider threat may increase. Insiders may have financial motivations for stealing data, or be motivated to act maliciously when they feel their jobs are threatened.

In practice, these cases tend to be statistical outliers. In talking to other physical and information security professionals, companies are not seeing a real rise in incidents that are tied to the economy. Nevertheless, in my experience, these threats have been out there, and the uncertain economy is just one more reason that we need to raise the priority of shoring up our internal networks and security controls.

Another comment that I’ve heard is that employees that are kept in the loop, informed about changes in advance and that feel empowered, are less likely to pose a threat.

[Slide 4]

As companies expand into new markets domestically and abroad, this may expose gaps in security practices. Working in Europe, Asia and South America, companies face many cultural and legal hurdles.

Privacy laws in Europe, for example, are different and in many cases more strict than in the US.

In some cultures, intellectual property is not treated the same as we treat it in the US. It is a big concern when doing business in Asia, that engineering drawings be properly managed and protected, or you run the risk of seeing a tractor that you produce in your factory, roll out of that new factory down the street.

When we first started doing business at our tech center in India, many employees seemed to stay just long enough to get some training or to add to their resume, before they were out the door and working for a competitor.

In the US, there have been many regulations that have driven security change, in the past decade. PCI. HIPAA. Sarbanes-Oxley. The realities of global legal and cultural factors motivate us to develop new security controls and practices.

[Slide 5]

Let me just read some statistics, from the Verizon 2009 Data Breach Investigation Report.

In 2008 there were 285 million data records compromised. As you can tell from the news, this number isn't going down.

All industries suffer from data breaches, although threat vectors may vary significantly.

The growth of financial services companies (those that store and share consumer data or process large volumes of transactions) is on the rise, and along with new technologies and changes in the economy, the threat remains and it is real.

The insider threat still accounts for about 20% of all data lost. It may have seen a slight uptick recently, depending on which data you refer to.

Also, online data is most often the target, and increasingly the threat is coming through business partners.

This being said, the Gartner Group reports insider incidents actually make up about 70 percent of network espionage, although corporate security on average spends less than 30 percent of their budget on the insider threat.

My interpretation of all this is that, while the media focuses on the big breaches, lost or stolen laptops, data tapes and Internet hacking, those incidents are few and far between. The insider threat poses a much more significant problem than we acknowledge.

[Slide 6]

There are some obvious ways that we can protect systems and data from the insider threat. I'll list these here, and then cover them more on the following slides.

Proactive measures include vulnerability assessments, such as are required by the payment card industry. Proactive security policies and processes.

Reactive measures include incident response, forensics and intrusion detection.

These aren't in any particular order; I actually put them in this order so they would spell something out.

One comment I have heard repeated is that we need to pay attention to historical data. When we respond to an incident, we need to learn from it and address any gaps to improve our processes. At the same time, I guess this would say that gathering our data and producing good security metrics is valuable.

Encryption needs to be included on every security list, so I have it here. Data at rest and in motion needs to be protected. Most recently, this has included putting full-disk encryption on mobile devices and laptops, as well as establishing standard methods of encrypting file transfers and email.

The way we dealt with role-based access and authorized our users needs to have evolved from how we did it ten years ago. Sarbanes Oxley regulations require that those with access to sensitive types of data have their access reviewed periodically. This means instituting new control methods and testing those controls for efficacy.

Internal segmentation, using various means is in vogue again.

And last but certainly not least, educating the user remains a high priority in mitigating the insider threat.

[Slide 7]

I already mentioned that it's important to pay attention to employees. If you treat people right, and provide training, they are less likely to break the rules. Some people are just going to be a problem, and there's no way around that. Awareness training helps managers and other employees identify those that are potential risks, so you can hopefully avoid an incident.

If we consider our business partners, with access to our internal systems to also be "insiders", then we have to realize one big distinction between an employee and a non-employee is that we don't control or even have visibility to HR decisions at another company. Consider the scenario where a supplier lays off staff. Perhaps one of their employees had a strong authentication fob that came from your company, so even though they no longer had access to their company network, they could still log onto your systems and act in a malicious way, because YOU didn't know they just got FIRED, so you haven't had time to deactivate their access, and the other company didn't think to recover your fob as part of their termination process.

With your own employees, you can develop better processes to manage change, as they move from job to job or get hired or fired.

Regulations like SOX have forced us to develop quarterly or annual reviews of access rights, so some of these process improvements are in place at many companies and we are a lot farther ahead with our security processes than ten years ago.

[Slide 8]

As many security experts have been quoted as saying, you can never eliminate 100% of the risk. This is true with the insider threat, as well.

I have worked in both the government and industry sectors, and it seems that most people I've come across are good intentioned and well-meaning. They are willing to trust people and hold the door for someone who forgot their security badge. With the proper security awareness training, employees realize the implications of letting someone tailgate into the office, or of signing in for a friend. But, year after year, people click on emails that are pretty obviously fraudulent. As much as I want to be loved, I don't click on messages that proclaim their love for me at work. (At least not since 2000, when I last did that!)

The human factor is much harder to address than security architecture problems. However, there is a lot that we can do with technology, to keep honest people honest!

Risk management will help you analyze threats and spend security dollars where they can have the greatest effect. Often we see the problem as so big, we don't know where to begin. In my experience, starting simple and cheaply, focusing on the low-hanging fruit is the best way to start. This will clear out the risk that can be easily addressed, and help to prepare you for follow-on phases that are more expensive and complex. Taking a phased approach with technology also allows your management to decide how much they want to invest in responding to risk.

I've already mentioned the importance of encryption, and I just emphasize it again here. Of course, you need some strategy for encryption so people know what needs to be encrypted. If you don't know what's valuable, what exactly do you protect? It's prohibitively expensive to treat everything as classified data. One suggestion I'd give to companies struggling with this problem is to take a look at your disaster recovery planning documentation. High value systems with a low RTO should certainly be considered business-critical.

[Slide 9]

There are many tools that can be applied to managing the insider threat and protecting your data. These are some that I think need more attention in the next year or two, to keep ahead of the curve.

Data Loss Prevention can be expensive, and you will need to be able to identify the data you want to protect, but DLP with agents throughout your computing environment can be a good way to manage data, or at least log it. It can also be expensive, so, depending on your needs, you may find point solutions to have greater impact for a lower cost, to start off with. I have a big concern about engineering drawings, so that's where we started. Eventually, I expect that we'll deploy some kind of DLP solution, but we're not quite there yet.

You might think that Intrusion Detection is a good technology to apply to the insider threat, but I think that's a mistake. First off, it's very difficult to establish a strict baseline of what's normal in a large computing environment. You might be able to do that to a degree at the perimeter, but internally, it is much more difficult. The other concern is the volume of data you will need to sort through. If your tools is generating lots of data, but nobody is looking at it, then it's of no real value.

Just to mention one more technology that I think needs to get attention, and that's NAC. Maybe 2010 is going to be the "Year of NAC". I think NAC holds lots of promise, but on the far end of the spectrum, it can be very complex and expensive. I think breaking up access inside the company to computers based on their "role", makes sense. Not all office computers need to talk to shop floor computers or the server farms at the data center. We don't want vendors to plug into our network and gift us with a new virus. Non-compliant computers need to be restricted a lot more than those that meet all our standards. I support a phased approach to NAC, starting off at a high level, and increasing granularity over time.

[Slide 10]

In the past couple years, despite the down economy, security budgets have generally fared well as compared to other IT budgets. Even though we feel that there haven't been that many more incidents due to the economy, yet, the potential remains and the concern is there, so this may help to justify new projects, aimed at the insider threat.

Risk analysis helps to also justify new spending, and in fact we have seen some new projects approved this past year. The point is, good security isn't being stopped, just because the economy is poor. If anything, spending is scrutinized more, but proactive managers understand the risk posed by NOT spending where it is warranted.

Significant progress can be made by starting small, going after the "low-hanging fruit" and by sticking to the basic security tenants, such as security in depth to improve the efficacy of your control measures.

[Slide 11]

Once we've decided on new tools and processes, or if we just want to do a better job with what we have, we need to develop security metrics that are meaningful and improve our ability to mitigate the risks we've identified.

In some fashion, you probably will get more meaningful metrics if you improve the data you gather. For a long time, security metrics had been more of an art than a science. We need to move away from the WAG and gather useful security events. This means some kind of central database, so we can create reports and measure our success.

It's also important to have managers review the access of their users, application IDs, groups and so on, semi-annually. You need to view security risks from different perspectives. But, the bottom line is to pull out meaningful metrics that show the efficacy of your controls, so you can have a real impact on the problem and not just turn it into a "CYA" exercise.

[Slide 12]

In conclusion, this is a big topic and there's no single solution to the insider threat problem. This is not a new problem, but we need to take a fresh look at it, and see how new technologies we might be embracing: mobile devices, social networking, collaboration tools, remote access... and so on, change the paradigm.

Being proactive is always better than reacting to front page headlines.

Standard security rules, such as "security in depth" and solutions that include people, processes and tools apply to this problem as well.

And finally, don't feel that you need to break the bank to have an effect. The perimeter hasn't disappeared yet! If you work closely with the business as they develop new ways to innovate, you'll be able to proactively secure new technologies before they get introduced into your environment.

THANK YOU FOR YOUR TIME. THAT CONCLUDES MY PRESENTATION. I'D BE HAPPY TO ENTERTAIN QUESTIONS FROM THE AUDIENCE.