Malware: Just What You Need to Know

Produced by SearchEnterpriseDesktop.com

Presenter: Kevin Beaver

Sponsored by

Malware: Just What You Need to Know

This document is based on a Sunbelt Software/TechTarget webcast entitled “Malware: Just What You Need to Know.”

Molly Toffey: Hello and welcome to today's webcast, “Malware: Just What You Need To Know.” My name is Molly Toffey and I'll be your moderator. Joining me is Kevin Beaver. Kevin is an independent information security consultant, a keynote speaker, and an expert witness with Atlanta-based Principle Logic, where he specializes in performing independent security assessments. Kevin has authored and coauthored seven books on information security including, Hacking for Dummies and Hacking Wireless Networks for Dummies. He is also the creator and author of the Security On Wheels blog, an Information Security Audio Program that’s providing security learning for IT professionals on-the-go. Thanks for joining us, Kevin.

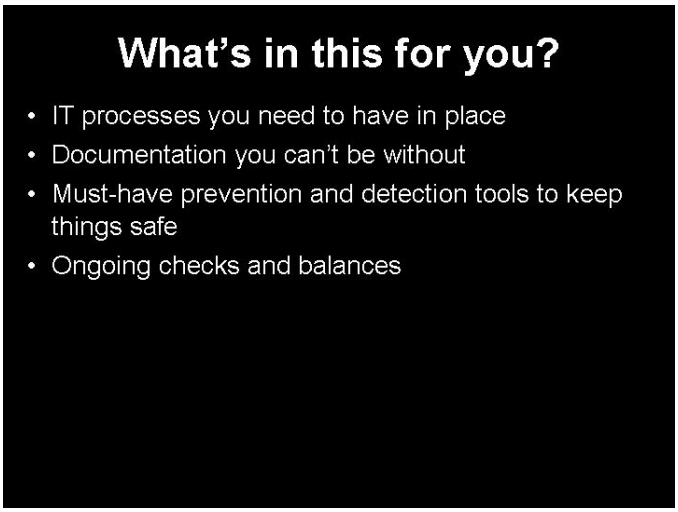
Kevin Beaver: Thanks for having me, Molly.

Molly Toffey: Whenever you are ready, Kevin, you may begin.

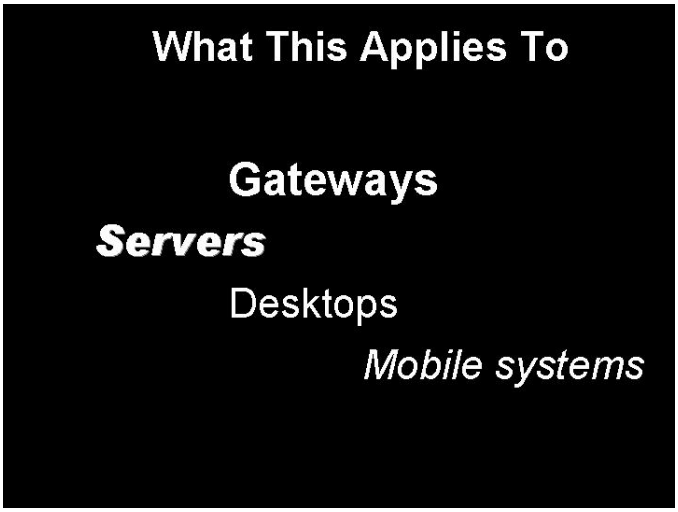
Kevin Beaver: Okay, thanks Molly. When was the last time you thought about malware protection? Or let me ask you this: when was the last time you thought about malware being a big risk for your network, your sensitive information, and your business overall. I'd be willing to guess that it's not so high on the priority list. You have some basic malware controls in place. You believe your users know what to look out for. And, after all, no big incidents occurred lately—am I right? You are not alone. Malware and malware protection have become an issue that we don’t think about that much any more. It's similar to thinking about passwords and patches. We know or we assume that the right controls are in place, and we don’t see the need to do anything differently. Whether you are a seasoned professional or just getting started in this area, I am going to share with you some insights and some tips regarding malware and, more specifically, malware protection that you may not have thought about or haven’t had the time to research and put in place. So let’s begin.

Over the years, I have learned all too well about the risks associated with malware through my own ignorance and through the mistakes of others. I've been working in IT for over 20 years and have been focusing on security for the past 14 years. I see a lot of poor implementation of anti-malware software. I see a lot of ignorance. On the bright side, all of these are problems that can be fixed.

Who can benefit from what I am talking about today? Network and security administrators and managers, compliance officers, architects, consultants, auditors, and forensic analysts. This includes anyone and everyone involved with computers, even down to the user level.

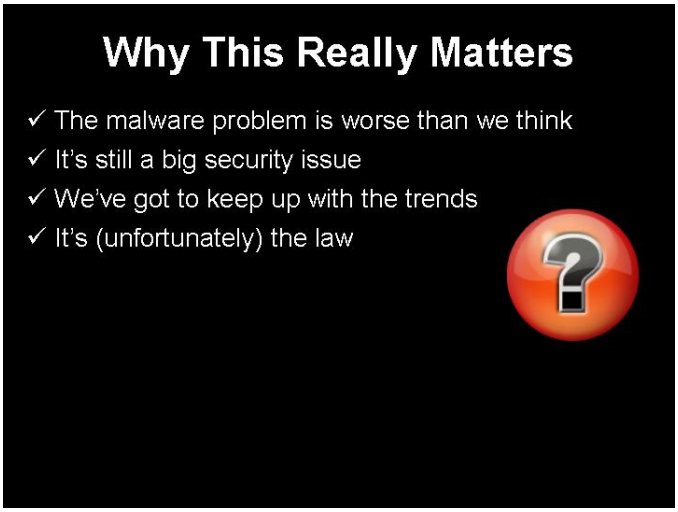


What's in this for you? What's in it for you are techniques, tools, and best practices for keeping a lid on the malware problem. These are things that are going to help you ensure that your time, money, and effort are all well spent. And even though many of us treat malware protection as a commodity, if we don't do these things the right way, these little bits of malicious code can turn into pretty serious information security issues.



The scope of this document is any computer that's plugged in and has a network connection, be it a internal LAN connection, an Internet connection, any type of mobile phone connection, wireless, and so on. Everything from network and e-mail gateways, be it offsite or onsite, in-house servers, all of your desktops, and all of your mobile devices scattered about.

Now that I have set the stage, let me share with you my experiences and the real substance behind malware protection and what it's going to take to make this happen in your environment.



Let me start by making a few points about why we should still care about malware protection. The biggest and most obvious issue is that malware is no longer a floppy disk or an e-mail problem. The attack surface for malware has become enormous. There are Java script-based malware attacks on social networking sites. There are the issues associated with USB devices, such as the FD worm and the variant of the QQPASS worm that was delivered for free on MP3 players given away by McDonald's in Japan. There are root kits that are becoming more prevalent, especially in Windows. We are faced with zero day attacks. There are distributed botnets, malware on our mobile devices. Attackers are becoming more and more clever. This is like an arms race. It's probably not going to end any time soon, if ever.

I had an experience with web-based malware recently. I was visiting a website that used to be legitimate, and it since has been taken over by criminals trying to push their fake anti-malware software. I was getting pop ups in my browser that I couldn't get rid of. Then after I clicked to close the window several times, it got to a point where it actually started downloading the executable to my system. I finally decided to kill the web browser process. I was using Firefox 3.0 and had pop ups blocked, but this malware still found a way around the built-in controls. This is something that my anti-malware protection never recognized. Imagine what could happen if a gullible user who is not up to speed on the latest problems actually allowed such a download to complete and then installed the software. Although we hear about malware in the media, I still think a lot of people aren't taking malware as seriously as they should. It's easy to go into this blindly. You can just install antivirus on the desktop and the e-mail server and let it do its thing. We can't approach this so haphazardly. If we do, odds are that we are going to get caught off guard. Things are difficult enough. There are the PCI, HIPAA, and other regulations that are mandating this type of protection, so it's not at all optional.

Finally, another point to drive this home is that the network security market posted some nice revenue gains in the second quarter of 2008. And the primary driver behind that was the growth of spam and malware. Apparently, businesses have to invest more and more in protective measures for these security problems.

Costly Mistakes

1. Trusting
2. Not knowing
3. Assuming
4. Overlooking
5. Depending
6. Believing
7. Hoping
8. Waiting
9. Assuming

There are some deadly mistakes that I see quite often. There is a lot happening on our own networks that we are often not aware of. In fact, it's easier to get a false sense of security, assuming that all is well in the world of IT as long as the basics are in place. Many people and mostly those in management believe they don't have anything a hacker would want and place their trust in a proactive network administrator. They claim to have good security technologies, that they have hardened their servers, that they are compliant, or that they have a policy against that. All in all, some very expensive mistakes are being made and even with something as "boring" as malware protection, the fact is that management trusts that all is well. People do not know or understand what's at risk. There is an assumption that compromises are highly visible. People are overlooking what the bad guys are doing. We are depending on users to protect and respond. We believe the security tools are the answer. Or we hope that security policies are the answer. We wait for a better time to address these security issues. We procrastinate. Or we make assumptions that "secure now" equals "secure always." And these assumptions are not good for business.

Common Issues I See

- ✓ Not valuing business assets
- ✓ Not protecting *every* possible system
- ✓ Wasting resources on full scans every day
- ✓ Multiple sets of policies and anti-malware tools
- ✓ Checklist audits (yep, AV software is installed!)
- ✓ Too much reliance on anti-malware tools
- ✓ Disable anti-malware
- ✓ Unprotected laptops

Let me share with you some malware-related issues I often see at my work performing security assessments. First, the main thing that I see is siloed and inconsistent security approaches. I see multiple teams responsible for multiple areas, and no one is talking to each other. I see one person responsible for malware protection, another person is responsible for operating system administration, another person is responsible for security, and so on. Case in point, I came across the situation not long ago where I found that the anti-malware software on a public kiosk-based computer not only had outdated antivirus, but the outdated antivirus software could also be disabled by anyone. Furthermore, there was no spyware or root kit protection. Not even a personal firewall was installed. This is problem enough when it takes place in a computer in the accounting office or on an IT admin system, but image the severity of this problem when

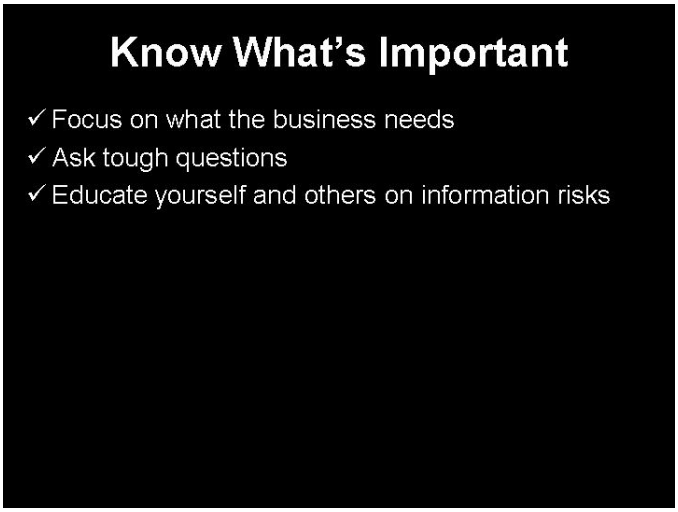
it takes place on a publicly assessable kiosk system. The problem in this particular situation is that no one had full accountability for the security of this kiosk. The load and the blame were spread across several people, and no one was accepting the responsibility to fix it. Similarly, I see people performing checklist security audits, for example, where someone claims that anti-virus software is installed. But they are not doing any in-depth security testing to find out how malware can enter the network, how it can be installed on systems like the kiosk computer I mentioned, and so on. Overall, they are not looking to see or to verify the effectiveness of the anti-malware measures.

My next point is about one of the most dangerous things that I see happening on networks today: giving users permission to respond to malware outbreaks and control their anti-virus software themselves without bringing anyone else in to help. Once users take incident response into their own hands, it's out of your control and anything can happen. This is likely to end up creating more work for you and more trouble for the business.

Finally, I am not seeing much more than plain old vanilla antivirus protection. Again, complacency is the culprit. And people are placing too much trust in the antivirus software vendor they have been using for 15 years, making assumptions that everything is protected the way that it should be.

When it comes to achieving and maintaining realistic malware protection, there is a lot to do. There is patch management, change management, security testing, software licensing, data backups, system monitoring, incident response, user education, and so on. We have to do this across multiple systems. We have the servers, the desktops, laptops, mobile devices, and network infrastructure systems.

How is anyone in IT or Security supposed to realistically keep up with all of this? The reality is that those people who are trying to do it all are not doing any of these things very well, because they typically are not using the right tools and the proper procedures for gaining control of their systems. They are getting caught up in the minutia. They also are not focusing on what's important to the business. So let me talk about that for a minute.

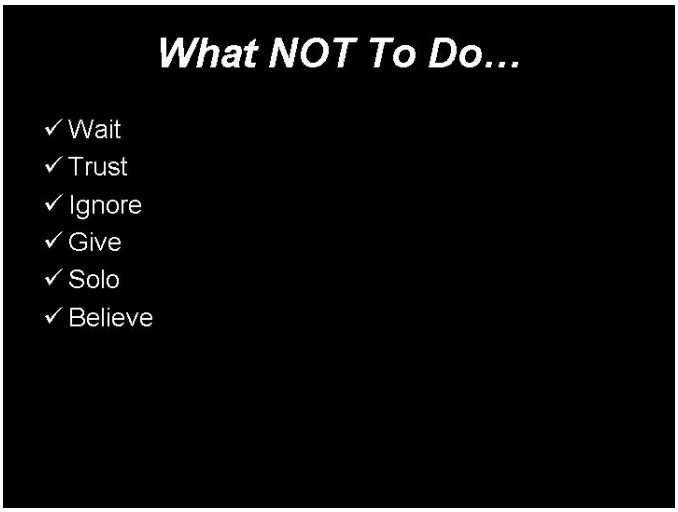


When it comes to any aspect of information security—be it policy enforcement, Web application testing, firewall management, or malware protection—we have to focus our time and energy on what's important to the business. We have to step back and ask what is it we are trying to accomplish here? Are we just trying to keep the junk out of our e-mail inboxes or are we taking a risk management approach and focusing very sharply on what it takes to make this aspect of information security worthwhile? And this is when being able to analyze security risks becomes a crucial part of your work.

The concept of information risk is something that you need to be using in every decision that you make. There is no need for a quantitative analysis, financial formulas, calculating the annualized loss expectancy, and so on. I am just talking about some basic qualitative analysis. When you do a qualitative analysis, you essentially determine your threats, which are basically an indication of intent to cause disruption, damage, or the loss that malware can do. You look at your vulnerabilities, which are weaknesses that can be maliciously exploited by a threat. And then you come up with your overall risk, which is the likelihood that damage or disruption is going to occur and then the impact that it's going to have on the business.

Malware threats exploit vulnerabilities in your systems, such as outdated software or gullible people, which creates risks for your business. You need to be able to tie information security controls and malware controls to business needs. In other words, this control satisfies this security or compliance requirement, which meets this business need. And that's the formula for making all this work.

So let me move on to my next point. Let's shift gears and start talking about how you can fix the problem of reactive security and reactive malware protection and turn it into something positive for your business to keep your systems protected from all the malware threats that you face.



Let me go ahead and talk about what not to do. Here is a list of six items of what you should not do when you go about implementing your security controls in the context of malware. First, don't wait for a better time to address the issue. When you put controls in place that work well, you can immediately reduce your business risks and lessen the chances of damage being done. So do it now. Second, don't trust that the right things are getting done. You have to verify. Just like with backups and other security tasks, I am always finding areas where malware protection is not loading, cleaning, or quarantining malware the right way. It's not being updated properly or it's just failing. So you have to keep on top of your applications and make sure they are doing what they need to be doing.

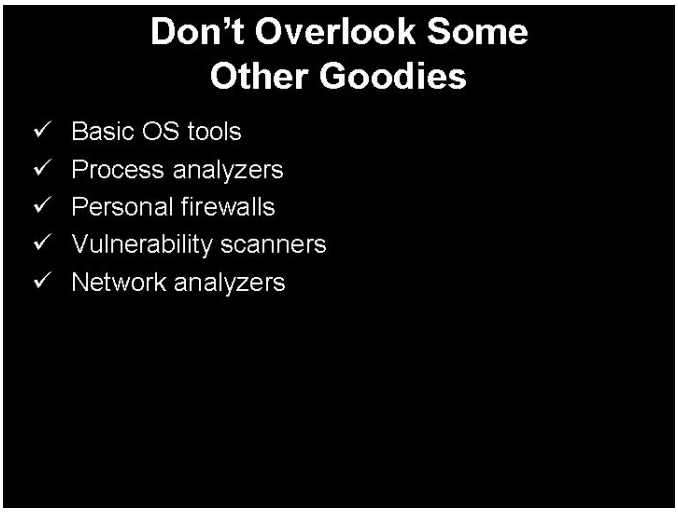
Third, don't ignore new malware tactics. Remember all the things that I mentioned with Web 2.0, Java script, USB, and other emerging issues. You can't afford to ignore it. Don't give users control or permission to respond. And also don't go with this alone. Malware protection is an information security issue and needs to be managed like one from the top down. And the only way that you are going to be able to gain control over your users is if you have the buy-in from management and you have a security committee that can back you up. And finally, don't believe that anti-malware tools are the one and only answer, which leads me to my next point about what to actually look for in your anti-malware tools.

Here are what I believe are positive traits of good anti-malware tools. In other words, things that you should look for when you talk to vendors and look into upgrading your existing software or ruling out anything new. First, it should be simple to administer. I recently had to get rid of the anti-malware product that I was using because it was too complicated to administer. I was making configuration mistakes that could have turned into real trouble in the future on my own network. Make sure that the software is centrally manageable. I still see workstations and servers that have standalone copies of antivirus and anti-spyware software. That can spell real trouble for any network that has more than three or four computers. You must be able to manage it centrally so you can get more control. Look for something that works away from the desktop if possible. I am not saying don't let it work on the desktop, but you also want to look at solutions that work at the server and gateway level, as well as something that doesn't rely on user intervention. Again, you don't want your users to be the enforcers. You don't want them to be the incident handlers.

Also, look for tools that integrate well with your other security controls. These tools can include active directory, event management logging systems, and so on. You are also going to want tools that have good reporting capabilities. Reporting is all the rage these days with compliance and management and trying to sell security. You need something that has some good reporting capabilities. Generally speaking, you want a tool or a set of tools that are right for your environment, so choose what fits best.

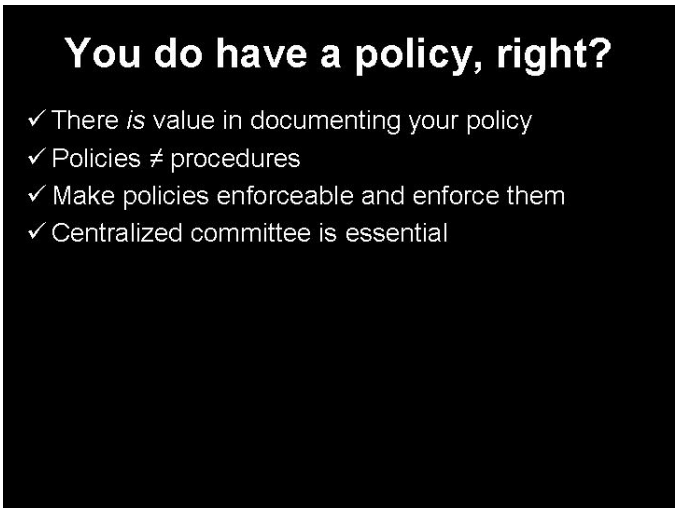
And always keep in mind that no matter what the sales people say, and no matter what the glossy marketing slicks portray, there is no single "best" anti-malware tool. Furthermore, you cannot rely on these tools completely. These anti-malware defenses and responses are not products that you can plug-and-play and forget. It's just like any other type of network or security administration that requires human

expertise, context, oversight, and proper procedures in addition to the right tools. If you are looking to upgrade your existing system or roll out a new anti-malware technology, my biggest recommendation for you is to always try before you buy. Most vendors allow you to try their products. You are going to want to see what you are getting into before you spend good money and a lot of effort and then end up realizing that it's not a good fit.

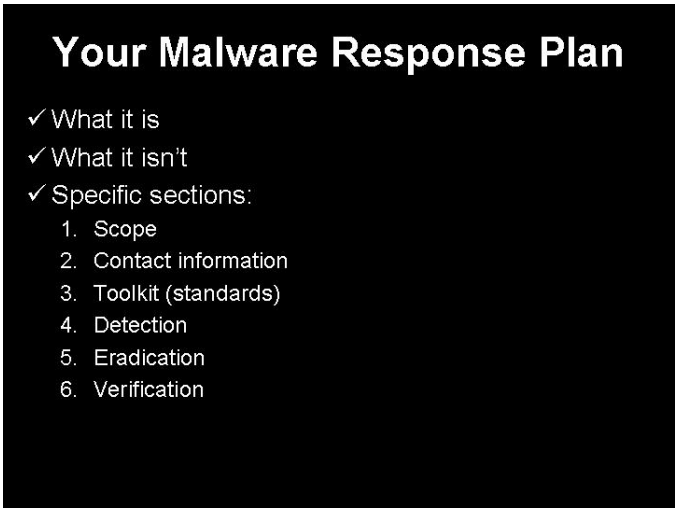


And when it comes to fighting malware, don't stop at anti-malware tools. There are some other tools that you are likely to have or can get for free or at a low cost to aid in your efforts. There are tools built right into Windows such as TaskList, the Windows management interface command line, Net, Netstat, and so on. There are also the Sys internals tools from Microsoft that everyone working with Windows needs to get to know. These can come in handy when it comes to analyzing malware infections and potentially even preventing them. Personal firewalls can help block malware infections and can even help with incident response. There are also vulnerability scanners, which can show a system vulnerability such as malware infections that you may not catch otherwise, such as open ports, faulty configurations, and susceptibility to denial of service attacks. These are all things that you wouldn't be able to determine otherwise. And then, finally, network analyzers. They can help you develop a baseline of your network activity and performance. They can help you troubleshoot network, operating system, and application problems that could just be malware infections in disguise. They can help you detect malware infections, such as high traffic volumes, unsupported or old protocols, odd information flows, and systems and applications that don't belong. They can also monitor malware behavior. If you suspect infection, during your incident handling and incident response, you could load up a network analyzer and see what's going on. These are good tools that you don't want to overlook.

If your network is more than just a handful of computers, you need to get other key people involved not only with your anti-malware initiatives but information security in general. Here are some people you may not have thought about that can help out when planning your malware controls. If there's ever an outbreak, they can help you respond. People at the management level—those in Compliance, HR, Legal, and PR—should be on a security committee.

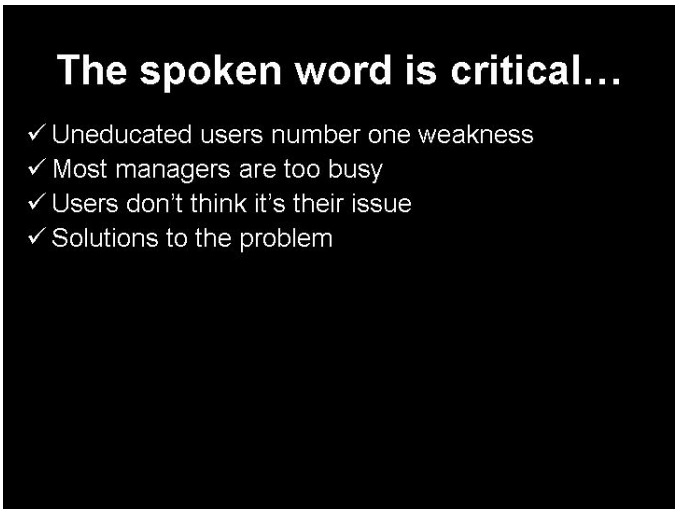


This leads me to security policies and specifically an anti-malware policy. There is value in documenting a policy. A good policy provides clear, concise statements covering a specific topic, in this case, malware protection. A good policy specifies how the organization handles malware protection. A good policy sets everyone's expectations. If there is ever a problem with someone doing the wrong thing, there is a safety net for the business, especially if compliance is an issue. The key with policies is not only to make sure they exist but to also make them enforceable and then actually enforce them. This is going to require getting other people involved—especially management—because they are the people who are going to be overseeing the business risks and issuing sanctions when violations occur. I can't say it enough: you have to get other people involved.



Let's talk about your response plan. Many people stop at the policy level, but integrating malware-related procedures into your incident response plan is something that you can't afford to overlook. Malware outbreaks are also security incidents. Some people say I know what to do when the time comes. But you don't want to have to rely on that attitude. You need some documented procedures for working through problems calmly and professionally. Your plan needs to include the definition of a malware outbreak. Is it on one system? Is it across the network? Is it suspected traffic that you are seeing with your network analyzer? How do you define that? It also outlines who does what task, when that task is performed, and

how that task is performed. Get your security committee involved, as well. I have listed the general sections you want to have in your incident response plan, which is the scope of what's covered, contact information of all the parties involved, your toolkits for anti-malware, any forensic tools, any other vulnerability scanning tools, your procedures for detection, procedures for eradication, and procedures for verification that all is well. The bottom line is that if we don't have a good plan for responding to malware outbreaks, they may get the best of us, make us look bad, and put sensitive information at risk.



It's one thing to document everything on paper but quite another to actually get the word out to users and management. In fact, uneducated and ignorant coworkers are the biggest problem we have when it comes to malware protection. Most managers are too busy to think about it. Others don't understand it and therefore ignore it. Users and regular employees don't want to be bothered with it. So what can you do? It's not as difficult as you might think. There are four steps. First, become a security evangelist. Make yourself known. Get the word out and keep the word out. Keep this information on the top of people's minds. Second, keep management in the know. You always want to keep them in the loop on your security initiatives, how your controls are working, and how their money is being spent, which is hopefully in a positive way. Third, remind everyone of the issues. This means not only standing up and preaching about security in a professional and calm way but also continuing to get the word out on a consistent basis. Put up trinkets around the office. Put posters in the break room. Set people's screen savers to remind them of what to do and what not to do. Provide training and show people what can happen when malware infections occur. Finally, show users how easy it is to be responsible. How easy it is to not open executable files attached to e-mails that they didn't solicit. How easy it is to just ignore solicitations, phishing e-mails, going to websites that they are not familiar with, and so on. This is pretty easy if you take the time and make the effort to put it in place.

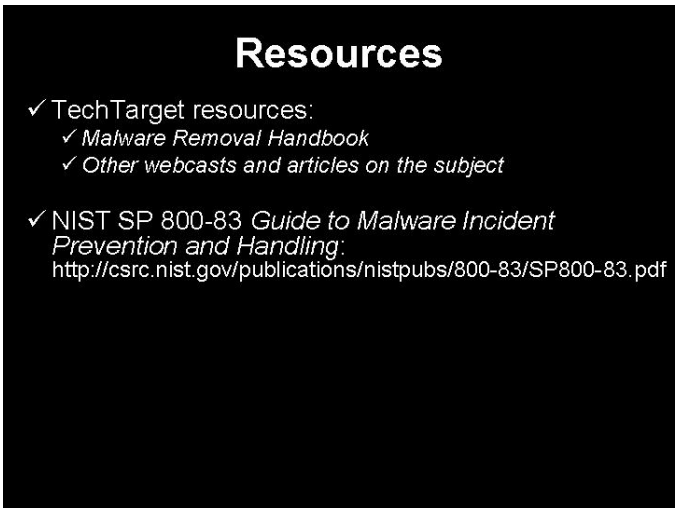
Here is the real key to making all this work: automate. Use technologies whenever and wherever you can to help enforce policies and keep your system safe. Automation is not only going to facilitate what you are trying to accomplish day in and day out, but it also remains vigilant when you can't be. You are not going to be in the office on a 24/7 basis, but your automated tools can. They can also help relieve a lot of the pains of managing security, regulatory requirements, and ongoing audits. These tools also facilitate change management tasks to close the loop and create sustainable and repeatable processes, which is a large part of what information security is all about.

Now let me conclude with a few slides to pull everything together.

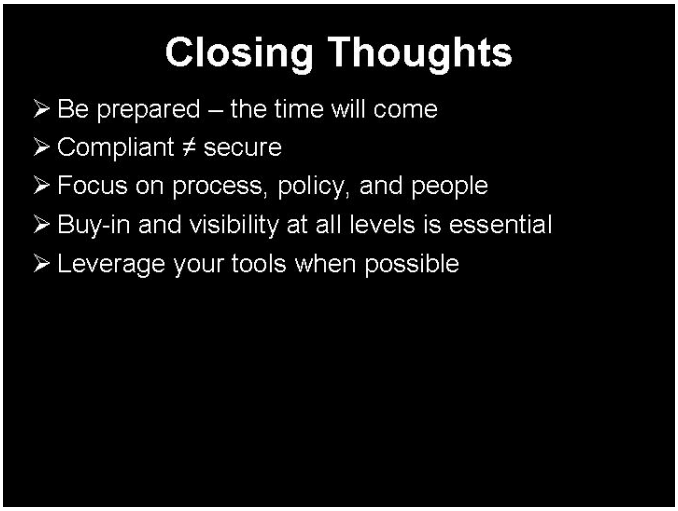
There are ten things you can do or start doing today to boost your malware protection and take things to the next level. Make malware protection less of a commodity and more of a top priority. Determine what there is to lose, understand your risks and your business needs, and document your policies and your incident response plan. Implement defenses at every possible layer, not just at the desktop. Do this at every layer possible. Don't forget about Windows. Hardening and patching your systems can go a long way toward protecting against malware outbreaks. So don't forget about the operating system. Keep everyone in the loop. Make sure that everyone is in the know of what to do, what not to do, and especially keep management informed of how things are working. Make sure that malware controls are being monitored and that response to incidents happens quickly.

Look at some of the newer technologies to keep web and mobile-based malware from affecting your organization. Find out where your weaknesses are by using proven, ethical, hacking techniques and good tools. Do not assume all is well just because malware protection is installed. Finally, always have a Plan

B. You may have to reload your system or systems to get rid of a problem, so keep your software media handy. When in doubt, reload.



Let me share a couple of resources with you where you can get more information on the subject. At TechTarget, you can find the Malware Removal Handbook that I wrote. If you don't have all these controls that I have talked about in place, I have provided some techniques, tools, and other resources for getting malware off of your systems. I have also done quite a few other webcasts and written quite a few other articles on the subject of malware defenses and offenses. There is also the NIST special publication 800-83, which is the Guide To Malware Incident Prevention And Handling. It's a great document and a good resource, so be sure to check that out. There is another resource I came across recently that is worth checking, out called Web Of Trust which is an IE and Firefox addon that basically warns users about dangerous and suspicious websites to help them avoid spyware, browser hijacking, and phishing. So check that out as well.



The malware problems need to be prevented rather than recovered from. Make that your top priority and primary focus. But even with the greatest controls and procedures in place, something bad can still happen. So you have to be prepared. Common sense is the best cure. Chuck Yeager once said, “You don't concentrate on risk, you concentrate on results. No risk is too great to prevent the necessary jobs from getting done.” What he said ties in nicely with what needs to be done to protect your systems from malware now and in the future. When it comes to malware protection, the difference between success and failure is decisiveness. Once you gather the facts, determine what's needed to make malware protection work in your environment and then make the decision to do what's right. You can't fail.

Molly Toffey: Thanks, Kevin. Once again, a quick thanks to our sponsor, Sunbelt Software. It was a pleasure, Kevin.

Kevin Beaver: Thank you, Molly.