3 WAYS SMALL BUSINESSES SABOTAGE THEIR CYBERSECURITY

3 ways small businesses sabotage their cybersecurity

By Michael Aguilar, Business Product Technical Lead, ESET North America

In my current role, I have dealt with a large number of businesses, from Fortune 500 companies to mom and pop shops. In many instances, the business model is similar; however, their practices are like speaking different languages.

As someone who has run a small business, I feel for the smaller companies and wanted to share a few bits of information in hopes of making your computing infrastructures a bit safer. I am also sharing mistakes I have encountered along the way so you do not have to make them with your small business. Below are the top three things that I see plaguing the small-to-medium business market—and ways you can proactively address these challenges.

1. Disaster Recovery

As those of us who work in computer security know, it is always imperative to have a way to go back in time. You hope for the best, plan for the worst, and always expect a curveball to be thrown when

you really do not need it—such as when trying to restore files due to failure, infection, or catastrophe (like flooding or weather instances that destroy, literally destroy, the machines). You would be surprised (or maybe you would not) to know the number of clients that I ask about their recovery techniques and they a) either have none or b) use something like Dropbox for recovery. Don't get me wrong—items like these small cloud services can be great for one or two files. However, if you need to restore all of June's payroll due to a server going down or incurring a Filecoder (Cryptowall) infection, it may not be your best option.

Numerous disaster recovery and backup techniques exist, such as tape drives, external hard drives that are rotated in case of one failing, and software that helps to make everything as seamless as possible. At ESET, we offer *StorageCraft* software as our backup and recovery software solution; it's easy to use and flexible in how you can use it to manage your file recovery.

It even has the ability to browse, use, and retrieve files from a browser if the entire site has gone dark. In case of emergency, having this kind of flexibility is key, especially if you are still trying to conduct business as servers are being rebuilt or a ransomware infection has locked

up your files. Forget the ransom; just restore your files and go home happy knowing that you are now back to green-light status. Do not be the person crying on the phone because your business has been encrypted with 2GB encryption and the files (along with your business) are effectively lost.

2. Antivirus or Endpoint Security

Everyone has antivirus, correct? You would think. Though Windows Defender does detect some malware and is an enhanced version of Microsoft Security Center, it still is not a top performer in regards to detections of malware, viruses, and spyware. In a *2015 AV Comparatives test*, Windows Defender missed about 8.6 percent of detections. While that is not a very large number, that one missed detection may be the difference between a downed infrastructure and you still having business to operate. I recommend that you choose a solid, paid antivirus solution to protect your computers. Freemium products, though enticing, normally lack some major functionality; hence the need for a paid license to utilize the entire suite.

ESET Endpoint Security products, which include versions with or without firewalls, earn very high ratings for detection and

performance from multiple testing companies and reviewers. ESET Endpoint Antivirus provides excellent basic protection, while ESET Endpoint Security includes additional features such as a firewall and web filtering. These products include ESET Remote Administrator so you can manage everything from a single console. You can easily add protection for file and mail servers with *ESET home office packages*.

If you only have a few machines, or want convenient protection for BYOD workers, consider a solution like *ESET Multi-Device Security*. It provides comprehensive protection for desktops, laptops and Androids with a single license.

Regardless of your chosen solution, once you have tested a few solutions, just make sure to install it on all of your machines. Another truly fascinating thing that I have encountered, more than once, are clients who havepaid for a license but have yet to install the applications, either due to time constraints or simply forgetting.

3. Policy and Procedure

Taking a page from large enterprise environments: Having a good policy and procedure in place is key. Though the business may be small, just advising your staff on how to operate can save time, money, and huge headaches by enabling them to perform well in their roles. In the smaller businesses I have talked to, jobs often have overlapping responsibilities. One person may be assigned to update web pages every week, but finds out that another person has taken care of it. The following week, it may be that both people skip the task, thinking the other person did it. In the end, nothing gets done.

Having clearly defined roles, and policies around those roles, will really help. There are many sites where you can find a framework of what you need; these include items like acceptable use policy for electronic devices, safety policies for those "in case of" scenarios, as well as disciplinary actions in case rules are not adhered to.

Granted, once you have the framework laid out, you will need to revisit it periodically as you notice items that may need reformatting or updating. But just having it will save you time and money in case something does go awry and you need to show that rules were not adhered to. If something goes catastrophically wrong, you will need to show that you had a safety policy in place to mitigate fallout due to an injury or loss of confidential data. Having it literally can save your business.

Michael Aguilar is a business product technical lead at ESET North America. He is studying for the CISSP exam and has a Security+ certification as well as a Usable Security certification from the University of Maryland Cyber Security Center via Coursera.org. He is currently responsible for working with large-scale clients for ESET North America and works with ESET developers, QA, and support engineers to resolve issues with clients in a quick and effective manner. Michael is active on Spiceworks and various security forums looking at new threat vectors and the best controls to mitigate those risks.

*For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit **www.eset.com**.*

ENJOY SAFER TECHNOLOGY®