IDEAS

THE TECH BEAT | BY JAMES HARDING

PREVENTING DISASTER

Let me tell you a horror story. Like all of the best horror stories, this is a true story (names have been changed out of respect for those involved).

Nov. 7, 2016, was a warm and sunny Monday. I arrived at work — along with many of my coworkers — thinking about the upcoming election and my day's agenda.

I began my shift as usual: setting up the store and checking my messages. The day couldn't have been more normal up until about 20 minutes after I sat down at my desk. That's when everything went black.

My software froze as if recoiling from a fatal blow while an insidious virus named for the God of Thunder ripped its way through our computer system — encrypting every image, program file and document it could find.

Within seconds, I was locked out of our printers. I had no access to my sales data, prospect records or even pricing. In fact, our register software (purchased from a NAMM member who sells POS software to tons of small music businesses) was particularly susceptible to the virus and — in a blink — it permanently ceased to function.

Protect your data from cyber intrusion before it's too late

Everything was just *gone*.

As the emotion of our situation subsided, we came to realize a harsh truth. Though the virus itself acted in a matter of a few minutes, the failures that led up to this tragedy began over a year ago. In fact, there were a myriad of ways we could have easily avoided Thor's wrath.

We thought we were as safe as anyone could be, but we were wrong. Sadly, it took a catastrophe for us to even consider our cyber vulnerabilities. But from the ashes of this attack, we've learned how to protect our business and — with the help of our intrepid IT team — ensure that a disaster like this will never happen to us again.

And how about you? Is your business disaster-proof? Are you sure? How old is your current backup plan? When was the last time you conducted a data security review? Do you even have one scheduled?

Take my advice. Even if you don't think you need one, conduct a proactive data security review and make sure your company information is safe. Here are 10 steps you can take to protect your business from a similar attack:

1. Plug it in. Power spikes can instantly fry your systems, but brown outs and "dirty power" can damage computers over time. Make sure each computer is plugged into a battery backup with surge protection and power filtering. APC makes some very reliable options.

2. Protect your machines. Not all anti-virus programs are the same. Some focus on less-secure "home" solutions.

I recommend a cloud-based, business class program like Bitdefender Endpoint Security. These programs offer better scanning options and professional support.

3. Protect your data. Modern viruses are designed to scan for and destroy backup drives. Don't risk it. Use a professional cloud service like Microsoft One Drive to protect your data and perform backups at regular (and appropriate) times during your business week.

Remember — not all cloud services are the same. Make sure yours is designed with business security in mind.

4. Implement web content filtering. Prevent employees from visiting inappropriate websites and picking up a virus or performance-slowing malware with a free service such as "OpenDNS."

5. Create a user account. Never use the administrator account on your computer. This master account has access to every bite of data and every service running on your machine.

Set up a user account and use it instead. Only use the administrator account when installing new software.

6. Set up automatic filters. With file sharing services like Dropbox or SendThisFile, you should never need to send or receive an email attachment (unless it's a PDF).

Have your IT team set up automatic filtering for risky attachments with extensions like .exe, .zip, .com, .bat, etc.

7. Buy smart. This was a big one for us as the register/accounting software we used at the time was built with a FoxBase database.

Make sure your critical software uses an SQL Database instead of a FoxBase database. SQL Databases are newer and much easier to repair in case of an emergency.

8. Click smart. Never open an attachment from someone you don't know — even if they claim to be sending you "the P.O. we discussed."

Spammers are constantly trying to fool you. Train your staff to demand that all attachments be sent via a service like Dropbox or sendthisfile.com.

9. Train your staff. Most businesses are vulnerable because their staff lacks data security training. Make sure your team knows how to close files out and shut programs down each night. Open files or programs will not back up.

10. Develop a plan. Work with your IT team to develop a "worst case scenario" plan that will protect your business data in case of disaster.

Update this plan at least once a year, and make sure you and your team aren't "getting soft" on data security. It requires constant focus.

THE AFTERMATH OF THOR

It's been eight months since Thor shattered our peaceful network, and we're still struggling to rebuild. The costs have been staggering — far more than we would have spent had we implemented the above 10 steps in advance.

We've had to pay for a host of data recovery services, new software installation and replacement hardware for the equipment that was damaged or destroyed by the virus. But the biggest expense has been the time we lost rebuilding our data. We're still re-entering paper invoices and counting every piece of inventory (from print music to pianos) in our stores.

At the time I'm writing this column, we still don't have an ETA for the completion of our recovery efforts.

At the conclusion of our investigation, we discovered that one of our business owners (who was logged into her administrator account) opened a legitimate-looking document attached to an email that appeared to be from one of our employees — only to discover (too late) that the email was a fake and the document was laced with a deadly computer virus.

It could have happened to anyone, but it didn't have to cause so much long-term destruction. Our failure as a company to remain current and vigilant with our data security protocols left us vulnerable to Thor's wrath, and we have been paying for it ever since.

Don't leave your business at risk. Viruses and ransomware like Thor are on the rise around the world, and the chances that you could face a disaster like ours increases daily.

No matter how secure you think you are, you owe it to yourself (and to your staff) to review your data security plan.

Make sure your business is as safe as you can make it because, as we have learned, in cyberspace, no one can hear you scream. **MI**

James Harding is the president of Gist Piano Center, a freelance web designer, pianist and avid blogger. Email him at jharding@gistpianocenter.com.