ENGLISH 101

By Jeff English, CFEE

RISK MANAGEMENT
Protecting More Than What You Think is a Risk

When someone thinks of risk management, the term is normally associated with preventing injury on an event venue. Trip and fall, bag checks, lost children and golf carts are all parts of a normal risk management plan. What I'll be covering today is a very different, but very real threat to festivals & events, along with every other small business across this planet of ours.

Seven years ago I was hired at the Kentucky Derby Festival to serve as legal counsel and to supervise our merchandise team and the Kentucky Derby Festival Foundation. Part of my job description, for whatever reason, also included supervising our IT infrastructure (Probably because I was the new guy and drew the short straw!).

Of everything I do at KDF, managing IT can by far be the most challenging and perplexing. I'm a lawyer by trade and have no formal training on servers, software, IP addresses, firewalls, or virus attacks. I do a serviceable job fixing small things, but KDF farms the complex stuff to an outside contractor. Seven years ago, my primary focus was getting our hardware, printers, internet and software up to date and working. We had printers that wouldn't print, laptops that were outdated, a wireless system that at times felt as if it were bouncing off a network of Russian satellites, and an outdated server that would shut down for no apparent reason. I honestly never knew (and still don't know) what IT headache was going to come across my desk when I walked into the office.

Until about two months ago, I was feeling pretty good about myself and how things were going in my little IT world. Our systems were updated, I had just ordered fiber optic internet cable to be installed, and the phone calls from frustrated staff members were at an all time low. If things were too good to be true, it means they were because things proceeded to go straight to hell.

Have you ever heard of the Cryptolocker Virus, or its ugly step brother, the Key Holder Virus? If you watch The Good Wife, they did an entire show on the virus encrypting the law firm's files. These bugs are forms of what are called ransonware viruses. Ransomware works like this: An e-mail is sent to a staff member with an attachment. The e-mail is usually from someone they know, so the staff member opens the attachment. BAM! The virus is launched and it strikes without mercy. It encrypts all of your files and will not allow you to open any of them. A message is sent that demands payment of $500 in Bitcoin within 10 days or your files will be locked forever!

We've been hit twice. Once on November 19 and just recently on December 22. After countless hours of research, talking with experts, and doing everything possible to not pay the ransom, we've unfortunately been forced to pay it twice. There's literally no way to crack the code once the virus has hit.

So in terms of managing the risk to your entire server and financial data, what can be done to prevent these ransomware viruses from attacking; or even better, what are your options if it does strike? Here's what I've learned after a month of bad dreams and sleepless nights:

1. There is no software on the market that can fully prevent Cryptolocker or Key Holder from striking once the virus has been "invited" onto your system. That means someone must open an attachment or click on a link embedded in an e-mail for the virus to launch.
2. Staff education is the absolute most important element to preventing a virus attack. Make sure staff members are very careful when opening e-mails and attachments. If it looks fishy, don't open it. Many times the virus comes in the form of a UPS or FedEx e-mail with an attachment claiming to have tracking information. If the person did not ship anything with UPS or FedEx, logic tells you the e-mail is up to no good.
3. Crank your spam filter and firewall settings up to their highest possible settings. Exclude all .zip files from getting past your filters. These files often contain executable software and easily launch viruses.
4. Install Malwarebytes on every computer in your office and run a scan.
5. Make sure your back-up systems are secure. Whether it's a tape back-up or on the cloud (whatever the "cloud" is), your only option, other than paying the ransom, is to get your files back through a complete rebuild of your system through back-up files.

Even if your office follows some or all of what I've listed above, there's no guarantee it will prevent an attack.

When I first started at KDF I never considered IT to be a "risk" that needed to be assessed. With everything we do being saved on a digital platform, not having access to this data can cripple your office's ability to function. Where before I was stressed over making sure everything was running correctly, KDF has now joined the ranks of Target, Michael's, PlayStation, Xbox, and countless other companies focused on preventing hacker attacks. It's a never ending battle with no end in sight.

Best of luck out there!

Jeff English is the Sr. Vice President of Administration/General Counsel of the Kentucky Derby Festival. After graduating from Washburn University School of Law (Topeka, KS) in 2004, Jeff worked in politics and practiced law before joining the KDF staff. He is charged with overseeing all of Festival's legal issues and serving as its risk management officer. He also manages the Merchandise Department and the 501(c)3 not-for-profit Kentucky Derby Festival Foundation.