Vol. 12, No. 1 2021

OutReach

A Christian Brothers Services Publication

Caring for others is in their DNA

Featured stories...

Cybersecurity in the post-2020 world

It seems like every day we hear about another company being hacked, their data compromised, stolen and held for ransom. It is a situation that is growing worse, and the border between what can be considered optional and what is required in cybersecurity continues to change year over year. What was once considered optional only a year or two ago is now considered best practice, and deciding how best to guard against hackers can feel like walking a tightrope with your organization's assets hanging in the balance.

Even the most diligent organization can fall victim to a cyberattack, but there are precautions you can take to help minimize the odds of becoming a victim and to lessen the effects the attack has on your organization if you are victimized. So what can you do now that will help you sleep better at night? As we continue to adapt to this ever-changing, post-2020 world, we will explore a cybersecurity model that can work for any size organization.

A growing problem

2020 was a boom year for cybercriminals. With the pandemic causing everyone to be sent to "Work From Anywhere," bad actors shifted to focus on this shiny, brand new opportunity. While it was good for them, it was bad for the rest of us. How bad? FBI's Annual Internet Crime Complaint Center Report (IC3), which includes citizens and businesses reporting crime, received a record number of complaints from the American public in 2020: 791,790, with reported losses exceeding $4.1 billion. This represents a 69% increase in total complaints from 2019. Business E-mail Compromise (BEC) schemes continued to be the costliest with 19,369 complaints with an adjusted loss of approximately $1.8 billion. Phishing scams were also prominent, with 241,342 complaints, totaling adjusted losses of $54 million. The number of ransomware incidents also continues to rise, with 2,474 incidents reported in 2020.

Over the past five years, a total of 2,211,396 complaints with $13.3 billion in total losses were reported. However, the problem is even larger because this is only the reported number. A lot of people and organizations don't report these crimes out of embarrassment. The actual numbers are even larger, and they are growing every year.

How does cybercrime occur?

Cybercriminals are primarily gaining access to company data systems through phishing, vishing, smishing, and pharming attacks. These attacks, through email, cell phones and text messaging are the biggest threats to organizations right now. They can come disguised as BEC schemes, where employees think they are paying an invoice or the CEO is asking them for something. These attacks happen fast, before people think to check on the validity of the request. By the time they are checked, it is too late.

Another method is through a tech support fraud, where a message pops up from what looks like tech support from a company like Apple or Microsoft to help you find malware on your computer. In reality, they are looking to get a credit card or bank account number to steal money.

Perhaps the most insidious crime is ransomware. Ransomware is where a thief will get someone in your organization to click on an attachment in an email. While it appears to the person that nothing actually happened after they clicked, it only takes a second for bad software or malware to be installed on the computer. That malware will encrypt an entire hard drive, then a message will pop up on your screen that you will need to pay a ransom to unencrypt it. In its "2020 State of the Phish" report, Proofpoint, a leading cybersecurity and compliance company, found that of the companies hit with ransomware crimes, 34% agreed to pay the ransom. But even after you pay them, you can't count on the bad guy to live up to their word and give you back your data.

One of the best ways to ensure that you won't have to pay a ransom is to ensure you have good data backups. These backups should be off site and not online. This is because when ransomware is installed on a machine, one of the first things it will do is find where your backups are located and encrypt them too, so offline backups are a must.

Stopping successful attacks

Proofpoint's survey also found that 57% of the respondents in a survey reported a successful phishing attack in 2020. What can you do to stop them? Until recently, organizations focused only on creating better passwords or using passwords as an only defense, but prevention alone is not enough. We also have to get good at detection. At Christian Brothers Services, we changed our approach a number of years ago to assume the bad actor is already in our network, and we have to be able to detect them.

Your organization is only as strong as its weakest link, so teach your employees about the various types of attacks. Most people know what phishing and malware are, but they don't know about ransomware, vishing and smishing. These terms should be part of your employee security awareness education program. All it takes in any organization is one person to click on a link or an attachment in a phishing email, and your system is compromised.

With people working from home, another danger involves who has access to company-issued devices. A key finding in the Proofpoint survey is that in the past year, more than 50% of those who have work-issued devices granted access to their friends and family for non-work reasons. Even if your employees are trained not to click on links that may have malware, their family members may not be.

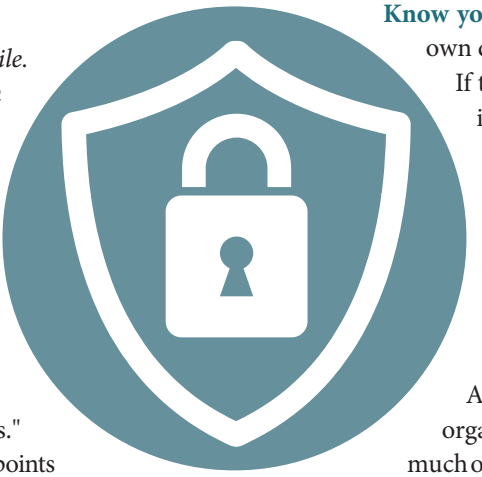
Mobile devices and "Man in the Middle" attacks

These issues for mobile workers are not going away. In its Mobile Security Report 2021, Check Point Software Technologies, a leading provider of cybersecurity solutions, shows almost every organization globally experienced a mobile malware attack during the past year. They forecast that 60% of the workforce will be completely mobile by 2024. Even with workers returning to the office post-pandemic, these numbers will continue to climb.

One of the best ways to ensure that you won't have to pay a ransom is to ensure you have good data backups. These backups should be off site and not online.

Their research also found:

- *COVID-19 is the new app attack premise*
- *Ransomware has gone mobile—it can be installed on iPhones, iPads and android devices*
- *Mobile devices are inherently vulnerable because people haven't focused security measures on them as much as desktops and laptops*
- *Mobile Device Management (MDM) is a powerful new attack vector. While mobile devices save us all time, attackers look to exploit weaknesses*
- *Major threat groups are focusing on mobile. Bad guys are looking to increase their return on investment by attacking mobile devices that may be less secure than laptops and desktops*



At the heart of mobile attacks are "man in the middle attacks." This type of attack occurs when bad actors try to get between the user and a network. For example, you try to join a Wi-Fi network at Starbucks and don't notice the network is spelled "Strbucks." Bad guys will make their bad wireless access points look like the legitimate business. As soon as you connect to their network, the bad guy is now between you and any site you were to visit. If you visit a banking site while on that network, your login credentials, and therefore, your finances could be exposed.

We may not think about it, but our phones and iPads have a lot of personal information stored on them. Whether it is pictures or contact lists, that information is valuable to an attacker and they will sell it or try to attack those people in your contact list to expand their attack base.

Protect your organization's assets

If all this alarms you, it should. These threats are not easing up; in fact, they are getting worse. The number of attackers seems to be growing and multiplying, while staying one step ahead of the rest of us. No one is off the radar, even faith-based organizations.

When you think about your organization and your cyber-risk exposures, determine what you want to protect. You have confidential information, proprietary information, and individually-identifiable information, which could be employee or donor or customer information, such as credit cards. If you were attacked, you would have to worry about loss of business and harm to your reputation as well as identity theft and lawsuits stemming from all these things.

In its 2021 Cyber Security Risk Report, Aon, a leading global professional services firm, touches on four areas to focus on to mitigate risk:

Remote strategies. Navigate the new exposure we all face in our rapid digital evolution. Only 40% of organizations report having adequate remote work strategies to manage this risk.

Ransomware. Only 31% of organizations report having adequate business resilience measures in place to deal with ransomware threats.

Know your partners. Since a lot of us don't house our own data anymore, we subcontract it out to vendors. If these vendors get hacked and our data is leaked, it doesn't absolve us of the responsibility to protect our data. Just 21% of organizations report having baseline measures in place to oversee critical suppliers and vendors.

Regulation. Less than two in five organizations (36%) report having adequate levels of data security preparedness.

Aon's main recommendation is to improve your organization to be a better risk. We can only spend so much on security, so we need to spend our money wisely.

The focus should be on:

- *Being proactive in our cyber security measures, including assessment, testing and practice improvement*
- *Privacy, including reviewing emerging privacy regulations and requirements*
- *Creating a cybersecurity culture, including training and education*
- *Preparedness for ransomware and business interruption*
- *Contracts with third-party vendors. Make sure there is wording in contracts to hold vendors responsible for data breaches*
- *Insurer transparency and communication*

The number of attackers seems to be growing and multiplying, while staying one step ahead of the rest of us. No one is off the radar, even faith-based organizations.

Balancing security and convenience

We all have to decide for ourselves if an IT risk management program is an optional component or a modern day requirement for our organizations. In the past, we worried about protecting and preventing; now we have to be concerned with detecting and analyzing because threats will get into our organizations if they are not already there. I have always said, there are two types of organizations: those that have had a data breach and those that don't know they have had a data breach. Once we have detected, we need to be able to respond and remediate as well.

Three things that will help you with your IT risk management program are:

Business Continuity Plan. You probably already have one and are operating it due to COVID-19.

Vendor Risk Management Program. As we all outsource more and more, focusing on our own missions, we depend on our vendors. Make sure they are dependable and protecting your data.

Cyber Liability Insurance Coverage. Bad things can and do happen, so it is best to be prepared. This coverage usually gives you access to other services, such as helping you detect the root cause and extent of the malware in your system, sending out notices, providing a year of credit monitoring to anyone who had their data breached, and providing you with legal defense.

Your cybersecurity program has to perform a balancing act between security and convenience. A system with too much security can become cumbersome to operate for your customers—think Department of Defense. If your system is too convenient and doesn't provide enough security measures, such as requiring complex passwords, your system can be easily compromised. Every organization has to find its happy medium.

What are the required elements for a modern day cybersecurity program? The answer depends on your organization's particular needs, but required elements today are:

- *Anti-virus, anti-malware software for every computer*
- *Strong, unique passwords for every website you visit and a password manager—encourage the use of pass phrases*
- *Encryption of all mobile devices and data in transit*
- *A secure email facility, especially if you are sending confidential information*
- *2-factor authentication on all devices—something you know (ID and password) and something you have (a code texted, phoned or emailed to you)*
- *Virtual Desktop Infrastructure (VDI)—Gives your employees their work desktop away from work while keeping them in the security bubble of the workplace infrastructure*
- *Inbound email spam, junk, malware filter*
- *Turn off Windows administrator rights—this allows only trusted administrators to install software on office computers and devices*
- *Infrastructure as a Service (IaaS) and Software as a Service (SaaS)—If you still have an on- premise data center or servers, you may want to consider moving it to the cloud and obtaining it as a service. With IaaS, none of us need to host our own servers any longer. SaaS is for software, such as QuickBooks as one example, which is hosted by Intuit, so you would go to that website and log in to your account.*
- *Secure off-site data backups*
- *Virtual Private Network (VPN)—creates a secure encrypted tunnel between your computer and your organization's computer system to prevent traffic from being intercepted*
- *Computer Security Awareness Program—employee education is paramount*
- *Monitor all devices 24x7x365 wherever they are located*

As another resource for your cybersecurity program, the Department of Labor recently released cybersecurity guidance, which can be found on the internet with a quick search that includes tips for hiring a service provider, cybersecurity program best practices, and online security tips.

A successful cybersecurity program will set policy, standards, procedures, and educate employees. These standards and procedures don't have to be complex. Write some things down on a sheet of paper—one page each for policy, standards and procedures. That gives you three pages to educate your employees about. Grow into it and expand it as you find it necessary.

Tom Drez is the Chief Information, Privacy and Security Officer for Christian Brothers Services.

CBS is a full-service IT & Website Services provider with a growing portfolio of products, services and preferred vendor relationships to assist Catholic organizations in meeting their IT goals and objectives fully and affordably.

If you have questions or would like guidance on online IT security measures or cloud hosting services, CBS ITS is here to assist you wherever it can. 800.807.0200 / customerservice@cbprograms.com

CHRISTIAN BROTHERS SERVICES

1205 Windham Parkway
Romeoville, IL 60446
800.807.0100 cbservices.org

Health ▪ Retirement ▪ Property/Casualty ▪ BMT Consulting ▪ IT & Website Services ▪ Catholic School Management ▪ Mission Advancement