# How Counties Can Protect Themselves Against Cyber Attacks

By W. Stuart Morgan III

Counties are attractive targets for hackers, and they are under attack!

After Georgetown County sustained a ransomware attack on January 20, the county worked hard to recover until receiving a clean bill of health 52 days later. Threatened by a growing number of cyber attacks in recent years, Lexington County continues to work hard to avoid one.

Both counties have learned lessons worth sharing.

### Lessons Georgetown County Has Learned

"Our county's cyber intrusion event occurred over the weekend when someone opened an email attachment," recalled Seth Housand, IT Director, Georgetown County. "The email itself did not set off any red flags within the email security filter at the time nor did it have any key idicators such as mispelled words, a strange email address or sense of urgency that you often look for in phishing emails.

"The only exception to that email was its attachment," Housand added. "Once that attachment was opened, its malicious payload was delivered. We became aware of the intrusion three days after the attack when alerts began and red flags went up because a server was rebooted off schedule and its services stopped. Upon investigation, we found a ransom note and all data had been encrypted."

> **"Our county's cyber intrusion occurred over the weekend when someone opened an email attachment. The email itself did not set off any red flegs … . The only exception to that email was its attachment. Once that attachment was opened, its malicious payload was delivered."**
> Seth Housand, IT Director, Georgetown County

That cyber attack destroyed all of Georgetown County's computer systems, and halted all of the county's virtual operations requiring Wi-Fi. The county paid a $10,000 deductible on its cyber attack insurance policy, which helped replace computer equipment. County Council also voted to approve a general fund increase of $140,000 to help pay for necessary network upgrades.

Jackie Broach, Georgetown County Public Information Officer (PIO), said hackers tried to gain access to county records, most of which were already public record. But they did access the social security numbers of about 50 county employees in one department that were stored on a computer, and some of the county's bank account information that was outdated and no longer used.

Georgetown County's leaders recognized that the attack would affect the public and county employees, and the importance of messaging immediately after the attack.

> **"The wide-ranging media interest in the days, weeks and months following the attack was more than a little surprising. Media interest was immediate, and the public had questions about how this could impact them and whether any of their private information was compromised."**
> Jackie Broach, Georgetown County PIO

"Our initial media statement went out early Monday morning, January 25, once initial stages of the investigation were conducted over the weekend," Broach said. "The wide-ranging media interest in the days, weeks and months following the attack was more than a little surprising. Media interest was immediate, and the public had questions about how this could impact them and whether any of their private information was compromised.

"My primary responsibility was to answer questions on how the cyber attack would affect the public, and to respond to the concerns of the public and media," she added. "After notifying county leadership, law enforcement and our county's cyber insurance company, I needed to tell the public what I could and be as honest and as transparent as I could about it."

Communicating externally with the public was one thing, but communicating internally with county staff was another, according to Broach.

Communication internally was significantly more difficult.

The county's administrative services/HR director set up regular virtual conferences on GoToMeeting every Monday, Wednesday and Friday morning to update departments on the latest developments. Communication was conducted virtually with department heads and other key county personnel until the county's computer systems were up and running again. Gmail accounts were set up and used for two weeks immediately after the cyber attack while the county's email system was inaccessible.

**" ... after the cyber attack, our IT staff served as the operational lead and other departments were forced to step back into more of a support role."**
Brandon Ellis, Director of Emergency Services,
Georgetown County

"The most difficult part about messaging following a cyber attack is figuring out how to answer questions when you are still trying to determine exactly what has been compromised," Broach said. "Because a huge part of my job is to be ready to communicate during disasters, such as hurricanes, and our county's cyber attack was very similar to that, my files were backed up, and all my equipment  was mobile. So, I was able to grab my stuff, move to the Emergency Operation Center (EOC) and keep working.

"The biggest issue for me was that I couldn't access my email," she added. "But I used the gmail address, which was set up for county use, and used that account to send out the initial news release to let people know that they could use my gmail address to contact me for the forseeable future."

Brandon Ellis, Director of Emergency Services, Georgetown County, facilitated the operation of the county's EOC after the cyber attack, and coordinated with emergency services agencies operating under the EOC umbrella. He also helped allocate emergency/disaster resources and coordinate with county leaders as they dealt with the attack.

Georgetown County's experience and approach to managing events like major floods, hurricanes and COVID-19 helped the county respond effectively and efficiently to the cyber attack.

"The all-hazards approach to our planning process allows our emergency response plans to be applicable to any and all emergency situations," Ellis explained. "In addition to our comprehensive emergency operations plan, which has a detailed appendix specifically for cyber incidents, we were also able to leverage our continuity of operations plan and our logistics plan to ensure that government operations continued while our county network was basically unavailable.

"Typically, during an emergency," he added, "our county's IT

*(Continued on next page)*

## How to Prepare for a Cyber Attack

There is nothing quite like suffering a cyber attack to make you rethink your county's plans and procedures for handling one.

Just ask Brandon Ellis, Director of Emergency Services, Georgetown County. He learned some lessons after his county sustained a cyber attack earlier this year that he believes could help other counties prepare for a cyber attack as well as any other catastrophic emergency or disaster.

Ellis emphasized that it is important to:

"**Be Flexible.** Staff members get in a routine and they enjoy technology when it is working. When it's not, they don't handle the situation as well. We were constantly preaching to our staff to be patient and be flexible. As we worked through the process we had to identify alternative methods to accomplish normally simple tasks. As systems came back online, they did not operate as fast as they may have previously due to added protection and scanning mechanisms.

"**Have a Backup Plan in Place and Know What It Is.** We have a very comprehensive continuity of operations plan (COOP) that each department reviews, updates, and contributes to annually. The first option was to activate this plan to continue operations but it was quickly identified that the information therein was not completely up to date for all departments. As we waded through this information and encountered challenges along the way, we successfully worked through them but our efficiency in navigating these issues and deficiencies would have been much better had we been provided the right information in the plan. The point: Review your plans and update them when requested. We do this so that the guesswork is out of the picture when an emergency occurs.

"**Have Backup or Alternative Systems.** We quickly learned that our emergency management department housed the majority of available surplus laptops, mifi devices, and cradlepoints within the county. We were able to manage the distribution of these resources to other departments using our resource allocation and tracking processes that we utilize for every other major emergency situation, and with great success.

"**Build Relationships.** From our emergency planning and coordination initiatives, we were fortunate enough to have some of our partner agencies from outside of county government immediately reaching out to provide assistance and resources. These relationships are based on years of great coordination and team building, and is a true testament to our whole community approach to emergency planning and response.

"We must approach every situation with an open mind and be willing to learn from it," Ellis said. "As a county, I think that we successfully did that after we discovered holes in our plans and procedures for handling a cyber attack when we suffered one earlier this year."

department is present in our EOC for activations but serves in a support capacity by fixing computer problems, resetting passwords, etc. But after the cyber attack, our IT staff served as the operational lead and other departments were forced to step back into more of a support role.”

> **“We have targets on our backs, and cyber attacks threaten everything from collecting money and reporting to state and federal agencies to paying bills and providing library services.”**
> Angela Christian, Georgetown County Administrator

Ellis admitted that the cyber attack exposed holes in his county’s plans and procedures for handling such an incident, but noted that it also provided an opportunity for Georgetown County to take steps to be better prepared to handle future incidents. To prepare for a cyber attack, he emphasized the importance of being flexible, having a backup plan and knowing that plan, having backup or alternative systems and building relationships before an emergency or a disaster. *(See* ***How to Prepare for a Cyber Attack****, P. 53)*

Angela Christian, Georgetown County Administrator, said counties across South Carolina are particularly vulnerable to cyber attacks because technology is integrated into the fabric of county operations.

“We have targets on our backs, and cyber attacks threaten everything, from collecting money and reporting to state and federal agencies to paying bills and providing library services,” Christian warned.

> **“In today’s world, it is not an option to have safe guards in place to protect against cyber attacks. It is a must.”**
> Debra Summers, Lexington County Council Member

“The cyber attack we suffered disrupted the basic services that we provide citizens every day,” she added. “Our buildings were not closed, however we had to do everything manually which required more time. Fortunately, services in public safety, personnel and financial records escaped with minimum problems. Once we were ready to go back online, we had to check and recheck every system to make sure we had clean data to restore.”

Christian recommended that counties spend money now to protect their computer networks from cyber attacks. She also recommended contacting law enforcement and seeking legal assistance as quickly as possible after sustaining a cyber attack.

“Remember, it’s a crime for someone to invade someone’s computer systems,” Christian emphasized. “So, bring in law enforcement and legal assistance early in the process so you can protect yourself and your citizens.

“Communicate often with your staff after a cyber attack,” she added, “and update them on the status of the attack to let them know what’s going on. Be diligent and educate county staff on the importance of security.”

## Lessons Lexington County Has Learned

Debra Summers, a Lexington County Council Member, said her county is blessed not to have suffered a cyber attack, and that she is convinced that it is worth whatever it costs to protect a county’s data against a cyber attack.

“In today’s world, it is not an option to have safeguards in place to protect against cyber attacks. It is a must,” Summers emphasized. “Updating equipment and software is expensive, but it is a necessary part of doing business, and it always will be.”

She recommended attending SCAC workshops and taking advantage of opportunities to learn about technologies that could protect your county against cyber attacks and make them more secure.

“I can’t stress enough the opportunities that the SCAC affords counties, as far as building relationships that provide you resources to reach out to,” Summers added. “Cyber attacks are real. Lexington County’s Information Technology Department knows this and protects our computer system as best it can. But we are also aware that there are things that are beyond our control. So, we must constantly test our system and watch for unual activity.”

Lexington County is unique because the county’s former IT director, Lynn Sturkie, now serves as county administrator. He has more than 30 years of computer and technical experience, including the eight years he previously served as the county’s IT director.

“Much of the information gathered and used in government is considered public data,” Sturkie noted. “However, we need to ensure the overall accuracy, completeness and consistency of data. In order to do so, we maintain processes, rules and standards to keep this data accurate and reliable. These levels of protection instill confidence in all users of government services.”

Lexington County’s cyber security has been threatened in recent

years, and it continues to be threatened despite the county's best efforts to protect itself against cyber attacks.

But Lexington County is not alone.

"More and more, county governments are becoming targets of ransomware and other threats," Sturkie said. "If you have email, Internet or utilize cloud services, there are constant risks of threats from both outside and inside your organization. So, it is important to remain vigilant about security, and to train your staff members how to recognize suspicious activity and how to prevent cyber attacks. Your staff is your best alert system, and security awareness is best fought with education and awareness."

> **"If you have email, Internet or utilize cloud services, there are constant risks of threats from both outside and inside your organizations. It is important to remain vigilant about security, and to train your staff members how to recognize suspicious actvitiy and how to prevent cyber attacks."**
> Lynn Sturkie, Lexington County Administrator

Lexington County provides structured training for all county employees to heighten their awareness of threats, and the appropriate actions they need to take to guard against them. Employees are required to take this training and retake it whenever necessary, and new employees are encouraged to take the training within the first week after they begin working.

Sturkie said counties need to be protected against external and internal threats. Staff members must also be able to access their information freely, but unauthorized persons should not be able to review, change or delete county information.

Lexington County has a Technology Services team that uses a number of approaches to secure data and systems from cyber attacks, including:

- Staff education and training to prevent breaches and reduce the number of computer viruses;
- Deployment of software and hardware to detect and eliminate viruses and malware while allowing and monitoring authorized access;
- Vulnerability scanning;
- Internal and external penetration testing by a third-party provider; and
- Annual testing of recovery procedures ensuring our capabilities to restore systems and data.

Sturkie recommended that county administrators support their technology teams if they have one, or create and support one if they do not. He also recommended that they use resources and services offered by other government organizations, and understand that they are not alone. There are many resources available to help protect county computer systems and data.

For a county to be sufficiently protected against cyber attacks, Sturkie said that it is important that:

1. Every employee be required to complete security awareness training
2. System access be authorized through an individual user ID and password
3. Third-Party security testing must include vulnerability scanning, external and internal penetration testing, web application penetration testing, wireless penetration testing, network database assessments, physical penetration testing and password audits.
4. An intrusion detection system must be used to monitor the network at all times
5. Security software patches must be applied weekly to user devices and monthly to servers, and procedures must be in place to make immediate security patches if a vulnerability is identified.
6. A full system backup must be performed weekly, retained per agreed upon user schedules, with incremental backups daily, and routine restore and recovery processes must be tested and verified annually.
7. Databases and portable devices must be encrypted.
8. Security policies and procedures must be defined for acceptable use, access control, internet use monitoring, and filtering, password security, wireless security, mobile computing and storage to name a few.

Sturkie offered one final piece of advice:

"Have a cyber security plan in place, exercise and test the plan often and make the necessary adjustments. Treat cyber security threats similar to other threats and have standard operating procedures in place and staff trained to address a cybersecurity threat.

"The threat," he emphasized, "is real."