Cyberattacks are booming. This is how the Butler County Sheriff became a victim

The email looked like any other when it arrived in the inbox of an employee at the Butler County Sheriff's Office in late 2020.

The sender's name was familiar, and the address seemed right. No big deal. Just one more email to answer before the end of the day.

Click.

And the hackers were in.

The sheriff's IT team spotted the breach and sprang into action. They intentionally crashed the system to limit the hackers' access to sensitive material, but that meant taking the entire department offline for almost a month.

With just one click, the sheriff's office became another victim of a global network of cyber thieves and scammers who launch more attacks and inflict more damage every year.

It also became, for almost an entire month, a low-tech operation reminiscent of the 1980s, requiring dispatchers to keep track of deputies and 911 calls with pens, paper cards and color-coded clips.

"It was the single most disruptive thing that I've seen happen in our office," said Anthony Dwyer, the chief deputy for Sheriff Richard Jones. "We're used to dealing with crisis, school shootings, rape, robbery, homicide. But not this."

What happened in Butler County in 2020 happens every day to businesses, individuals and government agencies around the world and close to home.

Cyberattacks have hit several Cincinnati businesses: 'Everybody is vulnerable'

Cincinnati's Museum Center and Underground Railroad Freedom Center shut down for weeks after a computer system breach in early March. Other victims in the past few years include Kroger, UC Health, Christ Hospital, Mount Healthy Schools, WKRC-TV owner Sinclair Broadcasting and Planning and Development Services of Kenton County.

A recent cyberattack on a Cincinnati Water Works contractor made it impossible for people to pay their bills online for almost two weeks at the end of March.

"Everybody is vulnerable," said Adam Lawson, the cyber supervisor for the FBI in Cincinnati and southern Ohio.

Cybercriminals know this better than anyone. Over the past five years, annual complaints to the FBI's Internet Crime Complaint Center more than doubled from about 300,000 to almost 850,000. Financial losses from cyberattacks and security breaches jumped from $1.4 billion to $6.9 billion over the same period.

Lawson said those figures are likely "the tip of the iceberg," because so many people and companies don't report security breaches, either because they don't know about them or don't want their clients and customers to know.

Though it's too early to measure the impact, Russia's invasion of Ukraine is raising concerns that more attacks are on the way. Russian hackers, some believed to be working for the Russian government, have been active for years and have targeted Ukraine and its western allies.

"The Russians are really good, probably the best in the world at cyberattacks," said John V. Franco, an engineering and applied science professor at the University of Cincinnati who studies cyber security.

"They have the potential for really screwing us up."

A cyberattack, then a ransom demand

It's not known if Russians are behind any of the recent security breaches in Greater Cincinnati, but attacks from overseas are frequent.

When the Butler County Sheriff's Office fell victim in 2020, officials there suspected the culprits were most likely based in Europe.

That's because the hackers eventually got in touch with them, demanding money for the return of data stolen from the sheriff's computer network. When they did, Dwyer said, the communications suggested English was not their first language.

At the time, though, identifying the home country of the attackers was low on the list of problems the sheriff's office needed to solve.

The first hurdle was figuring out how to stay in business. With most of the computer system down, sheriff's employees raided old supply cabinets for paper forms that had been in storage for more than two decades.

They used the old forms and started printing new ones so dispatchers could track their calls with pen and paper, instead of relying on computers. One of the dispatchers, who had been around since the 1980s, helped the others get the hang of it.

“It was working 20 years ago, and it worked again,” Dwyer said. “There were no major delays of any kind in dispatching.”

While deputies and dispatchers adapted to an old school, internet-free work environment, IT specialists set about trying to get the department back online.

Email phishing attacks are common because they work

They quickly spotted the source of the breach: A phishing attack that closely resembled a legitimate email from someone who regularly works with the agency. Once the employee opened an attachment or link in the email, the hacker gained access to the system.

According to the FBI, this kind of attack is by far the most common. Last year, the FBI recorded more than 320,000 phishing attacks, compared to 50,000 reports each of identity theft and personal data breaches.

Phishing is a favorite of hackers because it works. They don’t need every employee to open the phony email, only one.

“There are still people that don’t understand that you have to be cautious about emails,” Franco said.

Because computer networks are so connected, hackers often can gain access to tremendous amounts of data through a single breach. And when victims respond by shutting down their networks, everyone feels the pain.

That’s what happened at the Museum Center and Freedom Center, which had recently combined and upgraded their computer system. The new system meant everything from ticketing to lighting to visual displays at exhibits were tied into the same network.

Taking them down in early March pretty much shut down the whole operation.

“Within an hour, all systems were offline,” said Museum Center spokesman Cody Hefner. “You learn a lot about what systems are connected. It was pretty extensive.”

'It's about how much money they can make'

Finding the problem was the first step for the IT team in Butler County, but getting the system running again proved to be a bigger challenge.

If a software company wants to update a product or patch a glitch, it can do the job by sending out a link to customers. That won’t work after a hacker already has infiltrated a network.

To fix the problem at the sheriff’s office, the tech team had to physically touch every computer in the department.

Dwyer said it was an around-the-clock operation. Technicians cleared out a conference room and created a makeshift assembly line to handle every computer, from desktops and laptops to the computers used by deputies in their cruisers.

“They physically brought in units and scrubbed them and reinstalled everything from scratch,” Dwyer said.

At the same time, they assessed the damage caused by the breach. How far did the hackers get before the system crashed? Did they steal anything of value?

The hackers seemed to think so. When they contacted the sheriff’s office to demand payment, they sent “proof” of what they had and asked for money to get it back.

Turns out, the hackers wasted a lot of time downloading a huge folder containing old newspaper articles. They’d also grabbed a document showing what state IDs look like and another containing staff memos about promotions.

None of the files contained personal information of any value. The sheriff’s office refused to pay.

“They didn’t get anything off us, but there are private companies out there who will pay,” Dwyer said. “It’s a ransom operation.”

He said the sheriff’s office never found out who was behind the attack, but it appeared to be a profit-driven crime operation.

Lawson, the FBI supervisor, wouldn’t talk about Butler County or any specific cases. But he said criminals and criminal syndicates are among the most common forces behind cyberattacks, often using ransomware to encrypt files until the victim pays a fee.

That's what happened last February when hackers demanded $400,000 to release files they locked down at Planning and Development Services in Kenton County. The agency didn't pay and says it recovered most of its files, but some data and operations were compromised.

“It’s a business for them,” Lawson said. “It’s about how much money they can make.”

While the reasons for cyber attacks differ, the damage done is costly

Different attackers, though, have different motives. Those tied to governments, such as Russia, may be interested in espionage or destroying infrastructure. Others, known as hacktivists, may see themselves as ideological warriors fighting for a cause.

The hacker collective known as Anonymous, for example, declared cyberwar on Russia after the invasion of Ukraine and has claimed to have struck Russian media, banks and government institutions.

For those who are attacked, like the Butler County Sheriff’s Office, the motives matter less than the damage done.

Dwyer wouldn’t estimate the financial cost of the breach, but it altered every aspect of the office’s work for a month. And, he said, things weren’t completely back to normal until March 2021, about five months after the attack.

In response, Butler County officials bought new software and upgraded their system. But they knew that wouldn’t be enough.

Hackers target people as much as they target computers, so they needed to work on their staff, too. Everyone got new cyber security training and IT started sending out its own phishing emails to make sure the message was getting through.

The hope, Dwyer said, is that these new lessons will be less painful than the one everyone learned back in 2020.

“We take it very, very seriously,” he said.