Cyber Case Study

provided by Brooks Insurance Agency

City of Atlanta Ransomware Incident

In the spring of 2018, cybercriminals compromised several computer networks within Atlanta's City Hall to launch a ransomware attack. From there, the cybercriminals restricted access to a wide range of online platforms, municipal operations and databases—requiring a significant ransom to be paid in exchange for restoration. Nevertheless, the city of Atlanta refused to reward the cybercriminals and did not pay the ransom. As a result, the city took several months to recover from the incident, disrupting various government services for extended periods and costing millions of dollars in damage.

This incident has become known as one of the costliest cyberattacks to impact a local government, thus demonstrating the severity of ransomware threats. Upon reflection, there are a variety of cybersecurity lessons that organizations can learn by reviewing the details of this incident, its impact and the mistakes the city of Atlanta made along the way. Here's what your organization needs to know.

BROOKS INSURANCE AGENCY
A VENBROOK Company

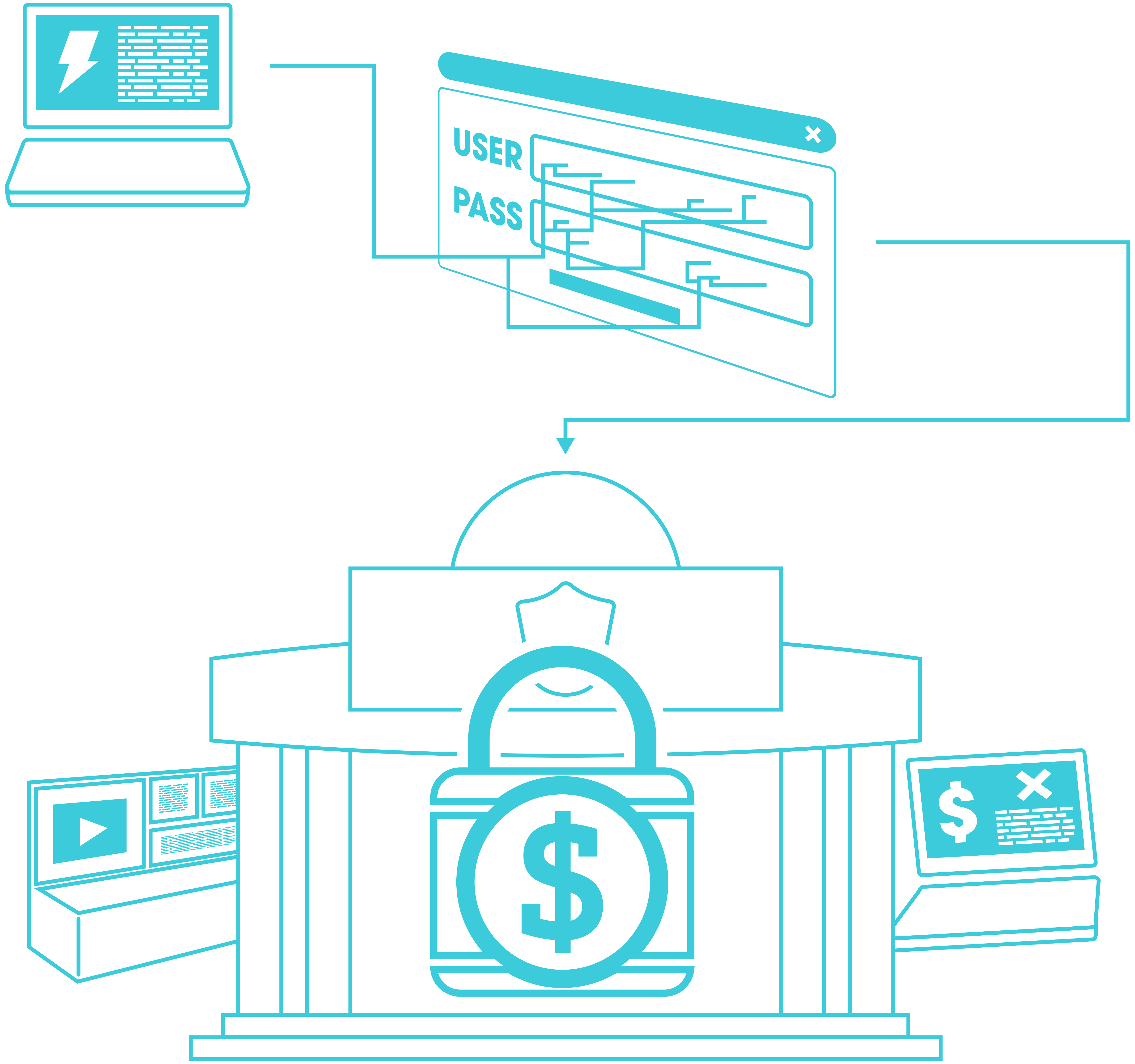
The Details

On March 22, 2018, cybercriminals utilized brute-force techniques to access several networks connected to Atlanta's City Hall. Using these techniques means that—rather than manipulating employees into exposing their network credentials for such access—the cybercriminals leveraged algorithmic password-cracking tactics in order to secure credentials. After obtaining access to government networks, the cybercriminals launched their attack using a customized form of malicious software known as SamSam ransomware.

The attack compromised critical technology and information across Atlanta, interrupting key municipal functions within several city departments. In particular, the incident disrupted online payment programs for various services (e.g., utilities, traffic tickets and business licenses or renewals) and a multitude of law enforcement operations, including warrant issuances, inmate processing protocols and court fee payments. Further, the Atlanta Police Department lost access to practically all of its archived in-vehicle video footage and even had to temporarily resort to writing incident reports by hand.

As part of the ransomware attack, the cybercriminals demanded the payment of over $50,000 in bitcoin before restoring any technology or information for the Atlanta government. However, the city refused to comply with the cybercriminals' demands; government officials did not want to reward the cybercriminals' behavior with payment, nor were they convinced that such a payment would result in restoration.

By not paying the ransom, the city was forced to recover from the attack on their own accord in the coming days, weeks and months. It took five days for the Atlanta government to regain access to critical technology. To prevent further cyber-related damages, the city kept the Wi-Fi at the Hartsfield-Jackson Atlanta International Airport disabled for 10 days following the incident until April 2. The government wasn't able to restore its online payment pro-grams until May, while local law enforcement couldn't fully resume digital operations until June.



An audit performed just two months prior to the incident stated that there were between **1,500 and 2,000** total vulnerabilities identified within the Atlanta government's digital operations and technology—suggesting the city had become **complacent** regarding cybersecurity.

The Impact

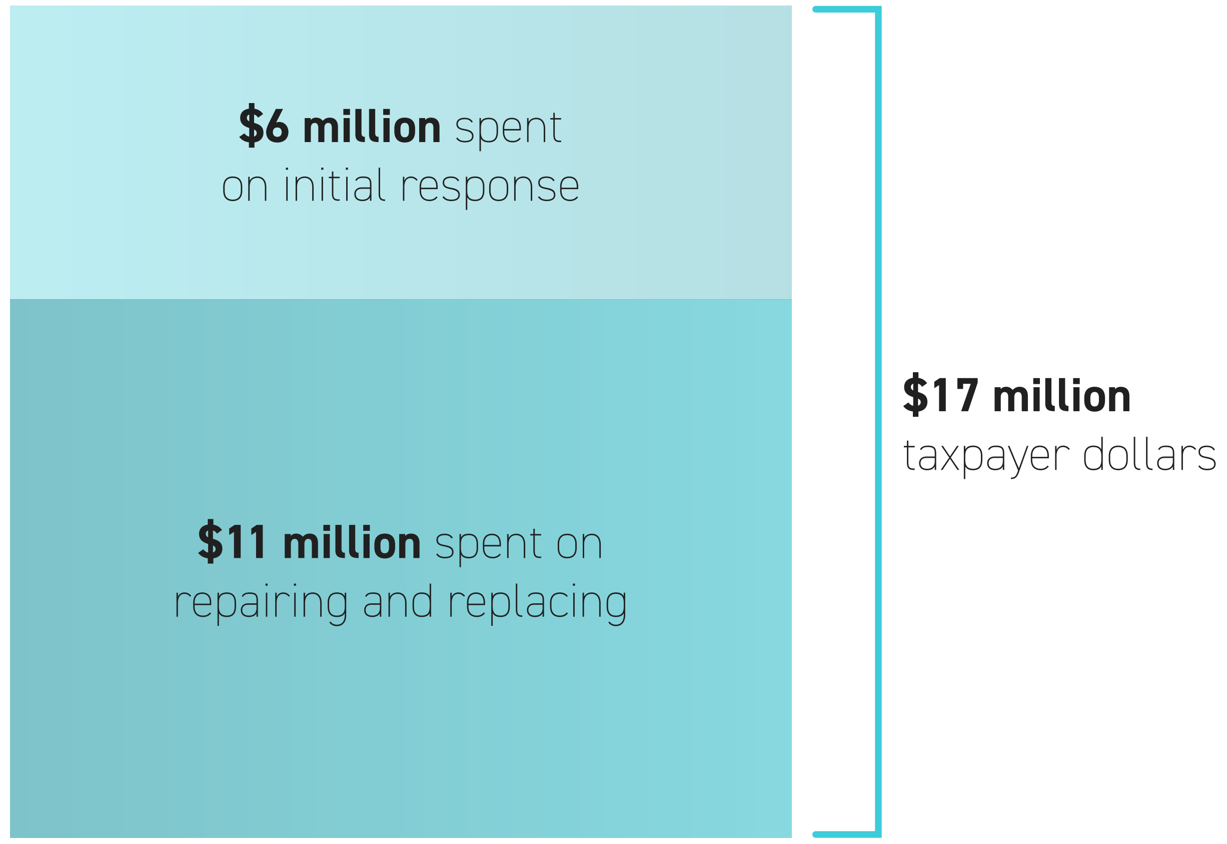
Following this large-scale ransomware attack, the Atlanta government encountered many consequences, including the following:

Disruption concerns

First, the incident interrupted many key functions within the Atlanta government, especially payment platforms and law enforcement services. Although the city was fortunate enough to maintain control of emergency response operations (e.g., 911 dispatch) and essential community offerings (e.g., water and electricity) throughout the attack, the disrupted municipal services still caused issues for both government employees and Atlanta residents. What's worse, many of these interruptions continued for extended periods as the city recovered from the incident, thus compounding concerns. While the Atlanta government made the right decision in not paying the ransom during this attack, it's important to note that doing so can often lead to a prolonged incident recovery process.

Recovery expenses

Next, the costs associated with recovering from the attack were severe. In total, the incident is estimated to have cost both the city and its taxpayers nearly $17 million. Breaking down these recovery expenses, the Atlanta government spent approximately $6 million in its initial response to the attack. This amount includes developing emergency contracts for assistance with recovering compromised technology; hiring a forensics team to investigate the incident further; consulting crisis communications specialists; and implementing necessary security upgrades. The remaining $11 million was spent repairing or replacing damaged government systems and technology, including desktops, laptops and smart devices. Additionally, certain information across law enforcement databases was permanently destroyed during the attack, representing an irreparable loss.



Reputational damage

Lastly, the Atlanta government faced widespread scrutiny for its outdated cyberinfrastructure after the incident. Some IT experts blamed the city's security failures for contributing to the severity of the attack. In fact, an audit performed just two months prior to the incident stated that there were between 1,500 and 2,000 total vulnerabilities identified within the Atlanta government's digital operations and technology—suggesting the city had become complacent regarding cybersecurity.

Lessons Learned

There are several cybersecurity takeaways from the Atlanta ransomware attack. Specifically, the incident emphasized these important lessons:

Effective access controls are critical.

Because this incident originally stemmed from brute-force methods, understanding how to defend against such tactics is crucial. Specifically, if the Atlanta government had had more stringent employee access controls in place when the attack occurred, the cybercriminals may have been stopped before they could infiltrate government networks and launch the ransomware. After all, it's much harder for cybercriminals to crack passwords and obtain access to networks when employees' credentials come with strict security protocols. Valuable access control tactics include the following:

- Instructing employees to develop complicated and unique passwords for their accounts in addition to changing these passwords on a routine schedule
- Implementing multifactor authentication measures that require employees to verify their identities in several ways (e.g., entering a password and answering a security question)
- Limiting employees' digital access solely to the technology, networks and data they need to perform their job responsibilities
- Segmenting different workplace networks to prevent all networks from being compromised if a single employee's credentials are exploited

Security software is worth it.

In addition to proper access controls, a wide range of security software could have helped the Atlanta government detect, mitigate and potentially prevent this attack. Although this software may seem like an expensive investment, it's well worth it to avoid devastating cyber incidents. Essential security software to consider includes network monitoring systems, data backup and encryption services, antivirus programs, endpoint detection products and patch management tools. This software should be utilized on all workplace technology and updated regularly.

Cyber incident response plans are necessary.

If the city had been prepared to respond to this incident, the recovery process likely could have been much faster and, subsequently, far less expensive than it was. Instead, the Atlanta government took several months to fully recover from this incident, ultimately increasing disruption concerns and compounding the overall costs of the attack. Such extended recovery issues emphasize how essential it is to have an effective cyber incident response plan in place. This type of plan can help an organization establish timely response protocols for remaining operational and mitigating losses in the event of a cyber event. A successful incident response plan should outline potential cyberattack scenarios, methods for maintaining key functions during these scenarios and the individuals responsible for doing so. It should be routinely reviewed through various activities—such as penetration testing and tabletop exercises—to ensure effectiveness and identify ongoing security gaps. Based on the results from these activities, the plan should be adjusted as needed.

Proper coverage can offer vital protection.

Finally, this attack made it clear that no organization—not even a local government—is immune to cyberattacks and subsequent losses. What's more, these events are increasing in both cost and frequency. That's why it's crucial to ensure adequate protection against cyber-related losses by securing proper coverage. Make sure your organization works with a trusted insurance professional when navigating these coverage decisions.

For more risk management guidance and insurance solutions, **contact us today.**