Data Spotlight

Presented by Winters-Oliver Insurance Agency

WINTERS-OLIVER
INSURANCE AGENCY, INC.

Cyberattacks Are a Leading Cause of Loss in Public Administration Sector

The federal, state and local government agencies that make up the public administration sector have become a top target for cybercriminals. These institutions are frequently attacked because they collect and store highly sensitive information and often lack proper cybersecurity controls due to limited budgets.

Review the following article for more information on the types of cyberthreats affecting the public administration sector, the frequency and severity of these losses in Advisen's database, and strategies for risk mitigation.

Cyberthreats

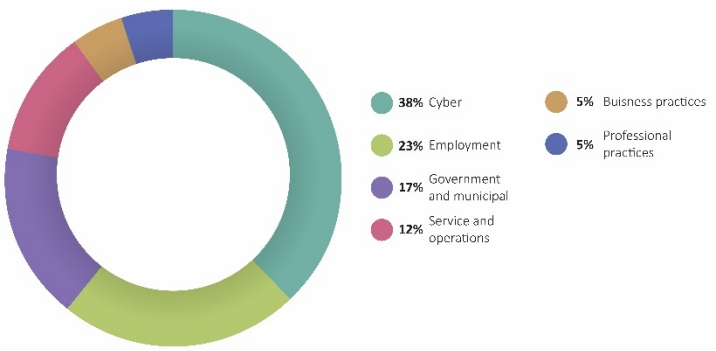
Cyberthreats that frequently impact public administration agencies include the following:

- Ransomware—With the installation of malware, this attack method is designed to take control of a user's system and prevent organizations from running essential functions until a ransom is paid. Recent research found the public administration sector was the target of nearly half of all ransomware attacks.
- State-sponsored cyberattacks—These attacks often involve one nation or nation-state attacking another government's systems to steal national secrets, sensitive information or money.
- Phishing—In phishing attacks, cybercriminals attempt to gain valuable personal information (i.e., credit card information, banking or routing numbers, security codes and more) by impersonating a legitimate person or institution via emails, phone calls or text messages.
- Hacktivism—Hacktivists are cybercriminals who typically engage in disruptive or damaging virtual activity on behalf of a political, social or religious cause. Individual or group hacktivists often work to expose fraud, reveal corporate wrongdoing or greed, draw attention to human rights violations, protest censorship or highlight other social injustices.
- Distributed denial-of-service attacks (DDoS) attacks—DDoS attacks occur when a cybercriminal attempts to interrupt an online service by flooding it with fake traffic. These attacks are especially common in public administration as a means to disrupt communication, send a political message or weaken governments.
- Insider threats—Internal breaches can originate from employee mistakes or irresponsible workers.

Advisen data

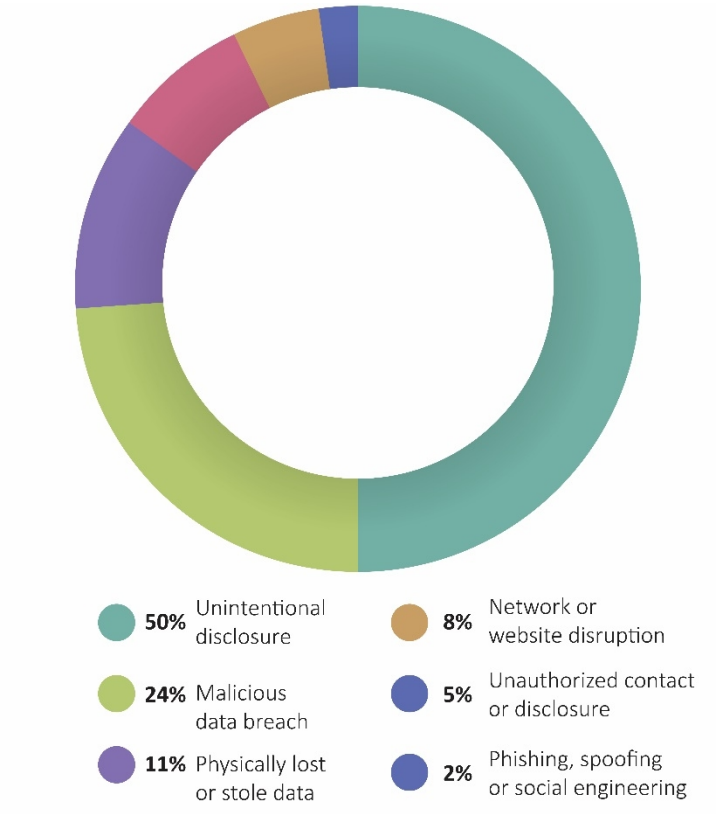
In an ever-evolving cyberthreat landscape, public administration institutions should understand the most common types of cyber losses, where attacks frequently originate and what types of data are being targeted. Consider the following:

Public Administration Losses by Category



Cyber incidents are the most frequent cause of loss in the public administration sector, accounting for 38% of losses in Advisen's database. Employment-related losses (i.e., discrimination, retaliation, wage and hour violations and wrongful termination) are second most frequent at 23%.

Cyber Losses in Public Administration by Type

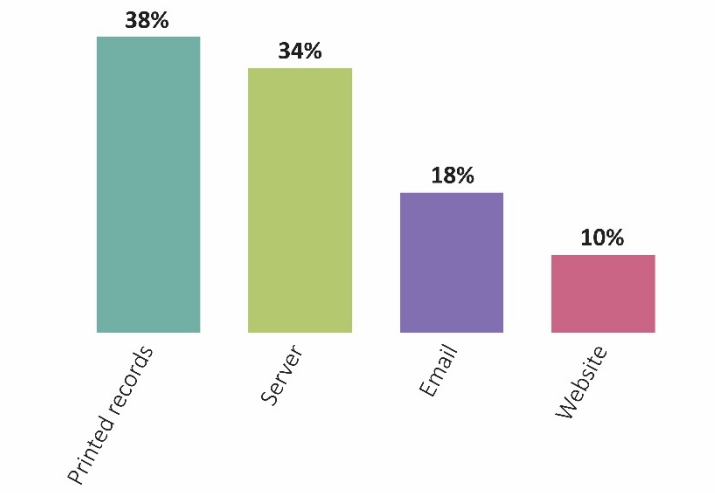


Unintentional disclosure accounts for half of all public administration cyber losses. This describes any instance in which sensitive information is copied, transmitted, viewed or stolen by an unauthorized individual.

Malicious data breaches account for nearly one-quarter (24%) of the remaining losses. This describes a cyber event in which someone purposefully accesses or shares sensitive information with the intent of causing harm.

Other common loss types for public administration include physically lost or stolen data (11%); network or website disruption (8%); unauthorized contact or disclosure (5%); and phishing, spoofing or social engineering (2%).

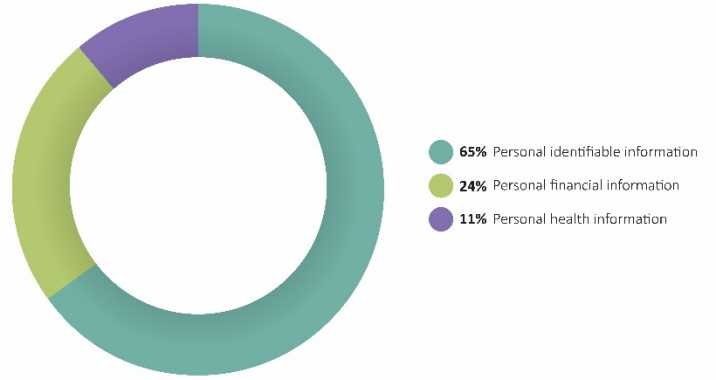
Cyber Losses in Public Administration by Source



Printed records are the most frequent source of cyber losses in public administration. These losses may be due to improperly stored records, leading to unauthorized access or theft, and are common in industries that lack the budget to properly store or dispose of physical records containing sensitive information.

Cyber losses that originate in the server are commonly DDoS attacks, which are designed to disrupt the flow of traffic to a website or force servers offline.

Cyber Losses in Public Administration by Information Accessed



Personal identifiable information—such as name, address, date of birth, Social Security number and email—was accessed in 65% of public administration cyber losses, whereas personal financial information (e.g., credit card information, bank account information and PIN numbers) was accessed in 24% of losses. Personal health information was the least frequently accessed.

Reducing the Risk

To help avoid and minimize cyber losses, public administration institutions should consider the following risk mitigation strategies:

- Train employees. Educate employees on safe cybersecurity practices. This may include training employees to identify and respond to attempted phishing attacks, encouraging employees to create strong email passwords, and ensuring employees are only using work emails for business functions.
- Create a cybersecurity plan. This plan should be reviewed annually to increase preparedness for new and emerging threats. When drafting a cybersecurity plan, make sure IT and security team members have a clear line for communication and collaboration with other teams.
- Consider remote work vulnerabilities. With short- or long-term adoption of a remote workforce, governmental agencies need to consider the vulnerabilities associated with nonwork devices, including cellphones. When possible, have dedicated devices such as laptops or tablets be used exclusively for business functions.
- Purchase proper coverage. It's critical to secure adequate insurance to help protect against cyber-related losses that may arise. It's best to consult a trusted insurance professional to discuss specific coverage needs.

Conclusion

As cybercriminals continue to heavily target the public administration sector, it's clear these institutions need to have strong plans in place to mitigate and respond to various cyberthreats. For more information, contact us today.