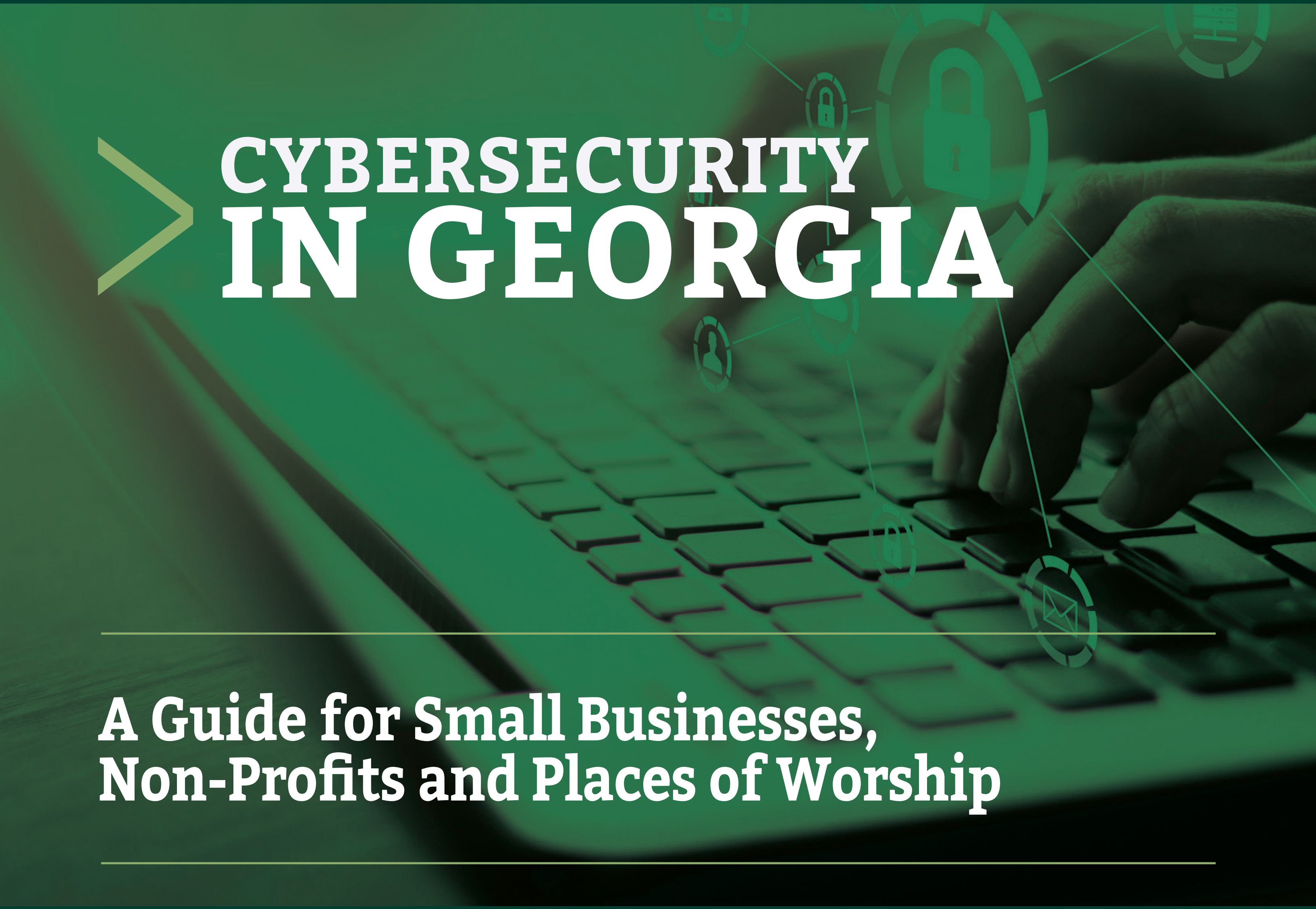
GEORGIA DEPARTMENT OF LAW
CONSUMER PROTECTION DIVISION



CYBERSECURITY IN GEORGIA

A Guide for Small Businesses, Non-Profits and Places of Worship

WHAT ARE THE THREATS?

There are a number of ways cybersecurity can be compromised.

PROTECT YOUR DATA AND NETWORK

Reduce your risk of a breach by controlling access to your network, protecting sensitive information and keeping systems and software up-to-date.

TRAIN EMPLOYEES

It is critical to establish security policies and educate all employees about cyber threats. Cybersecurity training should be continual– not just a one-time occurrence.

(internet network technology <ab2 . net>)
work technology <ab2 . net>)
p2p
SECURITY
technology <ab2 . net>)

TABLE OF CONTENTS

LETTER FROM THE ATTORNEY GENERAL

Dear Fellow Georgian:

Georgia's small-to-medium sized businesses, our non-profit community and religious organizations face unique challenges as technology is altering the way customers, clients and members are served. In so many ways this is positive, leading to more efficient and helpful methods to provide services and communicate to the public. But, we must also recognize that security breaches, hacking, phishing and other cyber threats are a reality in today's world.

Our Consumer Protection Division has developed this guide because we want to work with and support organizations to protect themselves and those they serve. This guide is intended to raise awareness of cyber issues and provide practical information that business owners and managers can use to ensure they are protecting their data and their clients' data.

We encourage you to review the material in this guide and communicate with those in your organization about the importance of cybersecurity and ways to reduce the likelihood and impact of cyber threats.

For additional information about the Consumer Protection Division, please visit consumer.ga.gov or call 404-458-3800.

Sincerely,

Christopher M. Carr
Attorney General of Georgia

INTRODUCTION

According to a study by the Ponemon Institute, 67% of small and medium-sized businesses in the United States were the victims of a cyber attack in 2018. Cyber attacks can have serious financial effects on the organization and the people they serve and may take many forms, from malware to social engineering. For example, in 2018, scammers posing as religious leaders of local Georgia churches sent emails to congregants asking them to make emergency donations through the purchase of iTunes gift cards. An orthopedics facility in Georgia was the victim of a phishing scam in 2018 that resulted in unauthorized access to an employee's email account containing the personal information of over 7,000 patients, including their names and other information typically found in a medical record. A smaller number of those records contained Social Security numbers and/or driver's license numbers.

The average cost of a cyber attack to small and medium-sized businesses is $383,365 ("2018 State of Cybersecurity in Small & Medium Size Businesses," Ponemon Institute). In addition, the average financial losses due to operational disruption are $1,562,124 *(ibid.)*, and the cost of damage or theft of IT assets and infrastructure is $1,426,422 on average *(ibid.)*. That does not take into account the potential loss of customers due to damage to your reputation. In fact, 60 percent of hacked small and medium-sized businesses go out of business after six months (National Cyber Security Alliance). Despite the fact that threats to small businesses from cybercrime continue to rise, barely half of small businesses have a cyber security plan in place (2018 Hiscox Small Business Cyber Risk Report).

Cybersecurity is crucial, but to be effective, it needs to go beyond the IT Department. Business owners and organizational leaders must ensure that cybersecurity policies and measures are implemented across the organization and that all employees are trained on how to recognize and avoid cyberattacks and protect sensitive information.

- The Georgia Department of Law's Consumer Protection Division created this guide to raise understanding and awareness of cybersecurity threats and highlight common industry best practices to keep your organization, and those you serve, protected.

consumer.ga.gov

WHAT ARE THE THREATS?

There are a number of ways cybersecurity can be compromised. Here are some common ways that cyber intrusion can occur:

✓ Data Breach

This occurs when private or sensitive information is disclosed without authorization.

✓ Hacking

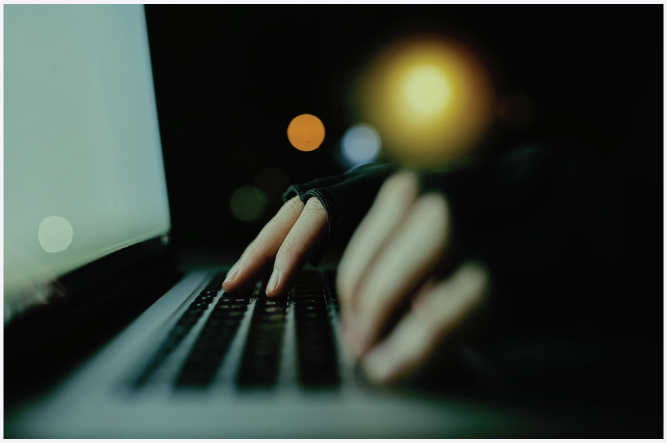
It occurs when a person exploits a weakness in a computer system and gains access to information.

✓ Phishing

Scammers impersonate a trusted entity to trick the recipient into providing sensitive information over email. Similar scams can occur over the phone ("vishing") and via text messaging ("smishing").

✓ Malware

This is software that damages or disables a computer and can infect your network. It hides within another application or file and can be downloaded accidentally by clicking on a suspicious link, pop-up ad or opening an email attachment.



✓ Ransomware

A type of malware that prevents victims from being able to use their computer until an expensive ransom is paid.

✓ DDoS attacks

Distributed denial-of-service or DDoS attacks target websites and online services with the goal of rendering them inoperable by flooding them with more traffic than the server or network can accommodate.

✓ Keylogger

This hardware or software is used by an attacker to capture each keystroke on a device.

✓ Issues from Unpatched Software

When software is not kept up-to-date, it is possible for malware to infiltrate the unpatched software and cause problems.

✓ Misconfiguration due to Human Error

Misconfigured cloud servers that include publicly accessible cloud storage, unsecured cloud databases and improperly secured rsync backups, or open internet connected network area storage devices can result in data being compromised.

✓ Tech Support Phone Scam

Con artists pose as representatives from a software company or security monitoring service and falsely claim to have detected a virus or other problem with a computer. The caller then directs the victim to download software that will allow the scammer to have remote access to the computer.

✓ Lost or Stolen Data

Unauthorized access to sensitive material may occur when personnel misplace a thumb drive or laptop.

TAKE INVENTORY

In order to secure your data, you first need to have a clear understanding of what types of sensitive information your organization maintains, where it is, how it flows through the organization and who has access to it. Examples of sensitive or personally identifying information are full names, Social Security numbers, credit card and financial information, tax documents, medical records/information, driver's license numbers, passport numbers, dates of birth and email addresses.

> **Don't keep sensitive data if there is not a legitimate need for it.**

TAKE STOCK OF:

- Computer systems
- Backup and storage systems
- Websites
- Laptops
- Employees' home PCs *(if used for work purposes)*
- Cell phones and tablets
- Flash drives
- Paper files
- Information shared with third-party vendors

WHAT IS BEING DONE WITH THE INFORMATION?

- How is it being used?
- How is it being stored?
- How is it being shared?
- How is it being protected?

HOW LONG IS SENSITIVE INFORMATION BEING RETAINED?

- Evaluate when sensitive data is destroyed. Update the destruction schedule as necessary to reduce the risk of exposure in the event of a breach.
- Ensure sensitive data is destroyed properly. Paper documents containing sensitive data should be shredded, and computer files should be securely wiped clean from hard drives and devices.

SCALE DOWN.

- Don't keep sensitive personally identifiably information if there is not a legitimate need for doing so. Better yet, if it isn't necessary, don't collect it in the first place.
- Delete software and apps you no longer use.
- Delete social media accounts you no longer use, as your records retention policies allow.
- Clean out old emails and empty deleted folders, as your records retention policies allow.
- Unsubscribe from e-newsletters, email alerts and updates you no longer read.

CONTROL ACCESS TO YOUR DATA

✓ Sensitive Data

Sensitive data should be accessible only to those employees who have a legitimate business need for it.

✓ Background Checks

Check references or do background checks before hiring employees who will have access to sensitive data.

✓ Strong Passwords

Require strong passwords of at least 12 characters that combine upper and lowercase letters, numbers and symbols.

✓ Change Passwords

Require employees to change passwords regularly.

✓ Limit Unsuccessful Log-ins

Limit the number of unsuccessful log-in attempts in order to limit password-guessing attacks.

✓ Multi-Factor Authentication

Require multi-factor authentication to access areas of your network containing sensitive information.

✓ Secure Remote Access

Establish secure remote access to your network. Never use public Wi-Fi networks to conduct company business unless you are using a secure connection, such as corporate VPN access or an SSL-protected web email server.

✓ Lock It Up

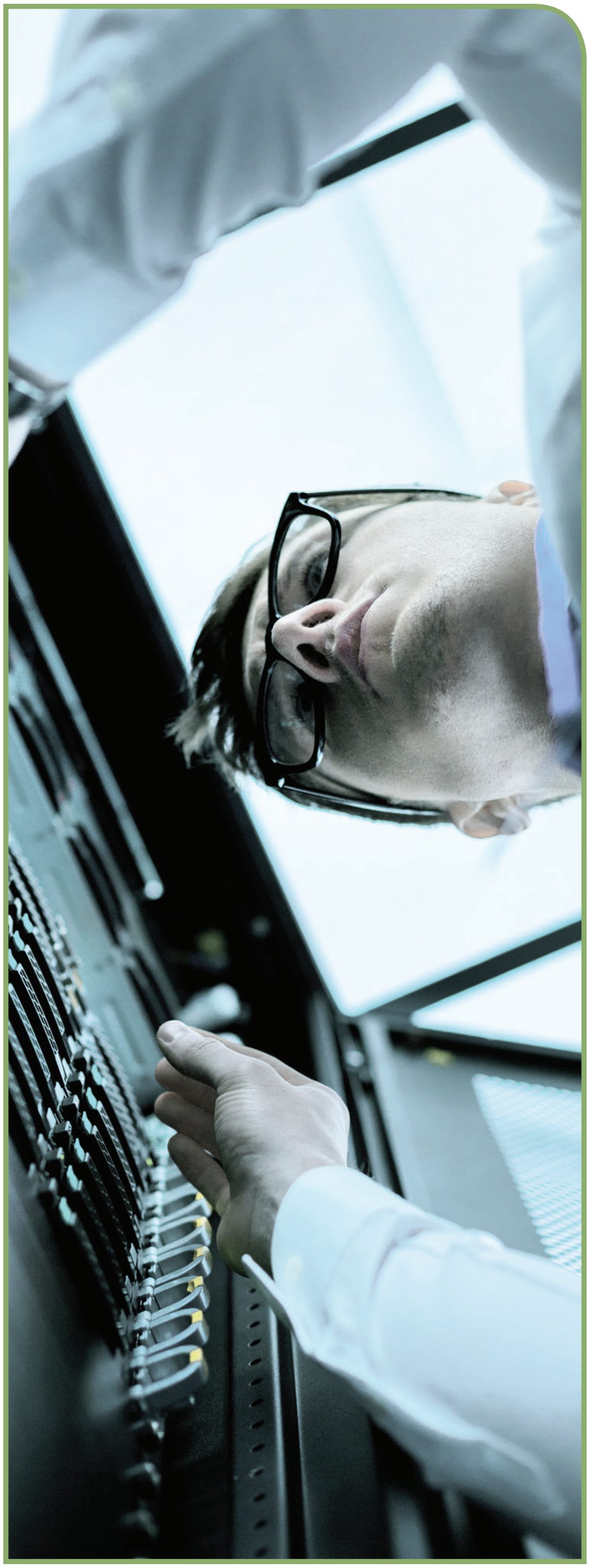
Paper files, thumb drives and back-ups containing sensitive data should be kept in a locked room or file cabinet.

✓ Termination Policies

Have policies in place so that when personnel leave your employ, their login privileges are terminated and their keys, access cards and identification cards are promptly collected.

✓ Limit Usage

Limit the usage of accounts with high privilege access.



PROTECT YOUR DATA AND NETWORK

Make sure your network is equipped with a firewall, pop-up blocker, anti-malware software and anti-virus software.

Back up data regularly.

Keep software, web browsers, operating systems, routers and mobile devices current with the latest updates and patches.

USE ENCRYPTION

Encrypt devices, drives, backup tapes, thumb drives and cloud storage solutions containing sensitive personal information.

Consider enabling full-disk encryption for laptops and other mobile devices that connect remotely to your network.

Use Transport Layer Security (TLS) encryption for your website to help protect your customers' privacy.

USE EMAIL AUTHENTICATION TECHNOLOGY

This technology prevents scammers from using your domain name to send emails that look like they're from your business and helps prevent phishing emails from reaching your company's inboxes in the first place.

BE ALERT FOR SUSPICIOUS ACTIVITY

Monitor your computers and network for unauthorized users, connections, software or USB devices.

Audit all active network accounts periodically for any unusual activity.

Monitor website traffic for any unusual activity.

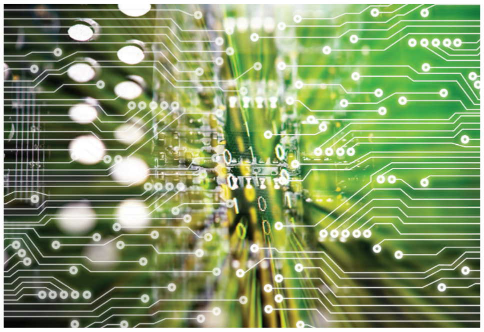
ENSURE VENDOR SECURITY FOR CLOUD SERVICES/SOFTWARE AS A SERVICE (SAAS)

Establish written security policies for the vendors with whom you share sensitive data.

Outline requirements for robust security controls, employee background checks and employee data security training.

Require vendors to perform up-to-date patching and vulnerability protection.

Establish processes to confirm that vendors are complying with the rules you've established.



Protect your wireless network.

- Once your router is set up, change the default name and password, turn off remote management and log out as the administrator.
- Make sure your router offers WPA2 or WPA3 encryption so that the information sent over your network cannot be read by outsiders.

Protect mobile devices.

- Use passwords for all devices.
- Set and use the locking feature.
- Avoid using mobile devices for banking, shopping or other sensitive transactions unless using a secure Wi-Fi connection, and then only use encrypted websites, which begin with "https" or "shttp" rather than just "http".
- Only use official app stores to download applications.
- Don't leave devices unattended in public places.

Secure social media accounts.

- Review the privacy and security settings on the accounts you use.
- Limit access to your organization's social media accounts to those whose job function requires it.
- Set policies as to what information can and cannot be shared via social media.

SECURE ONLINE PAYMENTS.

If your organization processes online payments, make sure you are working with an experienced online payment provider that makes security a priority. Choose a partner who is experienced with and complies with Payments Card Industry Data Security Standards (PCI DSS).

Your payment system should involve encryption, multi-factor authentication and an address verification system (AVS).

For additional media sanitization guidelines, see the NIST Special Publication 800-88 at: https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final

DISPOSE OF RECORDS SECURELY.

Georgia Law § 10-15-1 *et seq.* requires that business records containing sensitive information be disposed of properly. Before getting rid of such documents, shred them using a cross-cut shredder, which produces particles that are 1 mm x 5 mm.

Securely dispose of microfilm, microfiche or other reduced image photo negatives containing sensitive data by burning it until the residue is reduced to white ash.

Securely dispose of electronic devices. Simply deleting files or formatting a hard drive is not enough to prevent someone from recovering data using easy-to-come-by data recovery software. So, before disposing of computers, cell phones, tablets, copiers and fax machines, make sure you securely wipe the device clean and/or physically destroy it. *See detailed instructions in Appendix: How to Securely Wipe Devices Clean before Disposal.*

TRAIN EMPLOYEES

According to Ponemon Institute's "2018 State of Cybersecurity in Small & Medium Size Businesses," 60 percent of businesses cited negligent employees or contractors as the root cause of the data breaches they had experienced. That's why it is critical to establish security policies and educate all employees about cyber threats. Cybersecurity training should be continual–not just a one-time occurrence–so that employees stay current on the latest threats and remain vigilant.

Here are some key issues that should be addressed:

- **Password Safety.**
  Create strong, long passwords that combine upper and lowercase letters, numbers and symbols.

  Avoid using passwords such as your name, spouse's or child's name, date of birth, mother's maiden name or last four digits of your Social Security number. Don't use easily guessable passwords like "password," "12345" or "qwerty".

  Use a different password for each of your accounts so that if one is compromised, the hacker cannot log into your other accounts.

  Keep passwords in a safe place and do not share them with others.

- **Email and online threats.**
  Make sure employees are trained on how to recognize phishing and tech support scams and how to avoid downloading malware. Tips include:

  Be suspicious of emails from unknown senders and those containing odd requests or unusual spellings or characters.

  Never open email attachments or click on unfamiliar links unless you are sure the email is legitimate.

  Scammers may even include links that look credible at first glance, but if you hover your mouse over the link *(without clicking)*, you can see the actual hyperlinked address.

  Be very suspicious of requests to provide money, account numbers, passwords or PINs, even if the request appears to come from a colleague or vendor. When in doubt, confirm the request by placing a call to the colleague or vendor or run it by your supervisor or IT Department. Make sure you call the actual verified phone number, not the one provided in the email.

  If you get an outside email, call or pop-up ad claiming your computer has a problem, it's likely a scam. If you're worried your computer actually has a virus or issue, hang up. Do not respond to the email or call a number provided by the alleged scammer. Instead, contact your IT department or look up the legitimate phone number of your security software provider.

  Never grant anyone remote access to your computer.

  Establish rules for safe Internet browsing, including using only secure, encrypted websites when entering personal or financial information.

- **Unauthorized software.**
  Employees should understand that they are not allowed to download any unauthorized software, as this can make the company vulnerable to malicious software downloads.

- **Mobile devices and flash drives.**
  Employees should not use an unsecured Wi-Fi network for business purposes, such as checking work emails. When traveling, they should take care to guard laptops, tablets, cell phones and flash drives. Never plug unknown flash drives into your computer.

- **Handling sensitive data.**
  Employees should be educated on how to safely handle electronic and physical data containing sensitive information, such as Security numbers or financial account information, to avoid unauthorized access. Policies for safe storage, transmission and disposal of such data should be in place. Make sure employees who work from home follow these same policies.

- **Safeguarding Computers and Mobile Devices from Theft.**
  Establish policies for locking devices or keeping them in a secure place. Critical information should be backed up routinely and stored in a secure location.

- **Social Media Policy.**
  Establish policies for social media usage, such as which sites employees are allowed to use at work, who is allowed to create and maintain official company social media accounts, and the approval process for creating content. Employees should be prohibited from posting confidential company information, client information or trade secrets and from publicly discussing or speculating about company performance and unannounced business plans or acquisitions on any social media accounts, whether business or personal ones.

- **Visitors to your office.**
  Create a visitor policy that is suitable to the size and nature of your organization. It may include information about verifying a guest's credentials, whether visitors must be accompanied by an authorized employee, and which areas of the office are open to which types of guests. Some level of restricted access beyond the lobby is a common workplace practice.

- **Report suspicious activity.**
  Make sure employees know where to report suspicious emails, phone calls, unauthorized personnel or a lost device containing sensitive information. They should also understand how to recognize a legitimate warning message or alert in case of an actual security event.

PLAN AHEAD FOR A SECURITY BREACH

As a best practice, you should have an incident response plan in place already, so that if a security breach occurs you are poised to respond swiftly and effectively. This will help you limit the damage, facilitate the investigation and be prepared to communicate quickly to the press and to those whose data may have been compromised. You may want to include in your incident response plan different types of common scenarios, such as a lost device containing unencrypted data, an external data breach or ransomware, as well as potential incidents specific to your organization.

The Cybersecurity Unit of the U.S. Department of Justice's Computer Crime & Intellectual Property Section recommends that at a minimum, the plan should address:

- Who has decision-making responsibility for different elements of an organization's cyber incident response, including public communications, implementing security and mitigation measures, engaging with law enforcement and resolving legal questions;

- How to contact critical personnel at any time, day or night, and how to proceed if critical personnel are unreachable or unavailable;

- What mission-critical data, networks, assets or services should receive prioritized attention during an incident;

- How to contact and interact with other parties who host the organization's affected data and services (e.g., cloud storage service providers or commercial data centers);

- How to contact the organization's retained incident response firm or otherwise obtain incident response assistance, if needed;

- When and how to restore backed-up data, including measures for insuring the integrity of backed-up data before restoration;

- What criteria will be used to determine whether data owners, customers or partner organizations need to be notified if their data or networks may have been illegally accessed; and

- When and how to notify law enforcement and/or other government entities.

It is also a good idea to ensure that your legal counsel is familiar with the legal issues associated with cyber incidents.

Once you have created your plan, test and practice it regularly by conducting exercises. Be sure to keep the plan up-to-date to reflect changes in personnel and structure.

RESPONDING TO A SECURITY BREACH

Below are steps you should take and points of contact in the event that personal information may have been exposed.

SECURE YOUR OPERATIONS

Assemble a team of experts to conduct a comprehensive breach response. Depending on the size and nature of your business, this may include forensics, legal, information security, information technology, operations, human resources, communications, investor relations and management.

Consider hiring independent forensic investigators to help you determine the source and scope of the breach. They will capture forensic images of affected systems, collect and analyze evidence and outline remediation steps.

Consult with outside legal counsel with privacy and data security expertise.

Implement the recommended remedial measures as soon as possible.

Secure physical areas potentially related to the breach. Lock them and change access codes, if needed.

Stop additional data loss. Take all affected equipment offline immediately— but don't turn any machines off until the forensic experts arrive. If a hacker accessed login information, update user names and passwords of authorized users.

Do not destroy evidence. Don't destroy any forensic evidence in the course of your investigation and remediation.

Keep records and preserve potential evidence.

Keep logs, notes, records and data.

Keep or document any communications that might relate to the incident (e.g. threats, claims of credit, extortionate demands, suspicious calls, emails or other requests for information about the incident.

Record incident response steps.

FIX VULNERABILITIES

Service Providers - If service providers were involved, examine what personal information they can access and decide if you need to change their access privileges. Also, ensure your service providers are taking the necessary steps to prevent another breach from occurring.

Work with your forensics experts to analyze what happened.

Find out if encryption was enabled when the breach occurred.

Analyze backup data.

Review logs to determine who had access to the data at the time of the breach.

Determine the types of information compromised, the number of people affected and whether you have contact information for those people.

HAVE A COMMUNICATIONS PLAN

Create a comprehensive plan that reaches all affected employees, customers, investors, business partners and other stakeholders.

Don't make misleading statements about the breach or withhold key details that might help consumers protect themselves and their information.

Don't publicly share information that might put consumers at further risk.

Anticipate the questions that people will ask. Then, put the major questions and clear, plain-language answers on your website where they are easy to find.

RESPONDING TO A SECURITY BREACH (CONTINUED)

NOTIFY APPROPRIATE PARTIES

Although not required by Georgia law, it is a good business practice to notify law enforcement in the event of a security breach, especially if the incident was the result of criminal activity. Law enforcement can use tools and legal authorities that are unavailable to private entities to identify and apprehend whoever is responsible for the incident. Federal investigators can obtain data to trace an intrusion or attack to its source using search warrants, court orders and subpoenas. You can report a security breach to:

FBI field offices
www.fbi.gov/contact-us/field

U.S. Secret Service field offices
www.secretservice.gov/contact

Internet Crime Complaint Center
www.ic3.gov

Your local law enforcement

Notify affected individuals, businesses and organizations as soon as possible so that they can limit their exposure. If there is a possibility that such notification could jeopardize an investigation into the breach, consult with law enforcement and your legal counsel about how to proceed.

If the breach affects more than 10,000 people it needs to be reported to all credit reporting agencies.

Consider using letters, websites and toll-free numbers to communicate with people whose information may have been compromised.

Clearly describe what you know about the compromise. Include:

- How it happened
- What information was taken
- How the thieves have used the information (if you know)
- What actions you have taken to remedy the situation
- What actions you are taking to protect individuals, e.g. offering free credit monitoring services

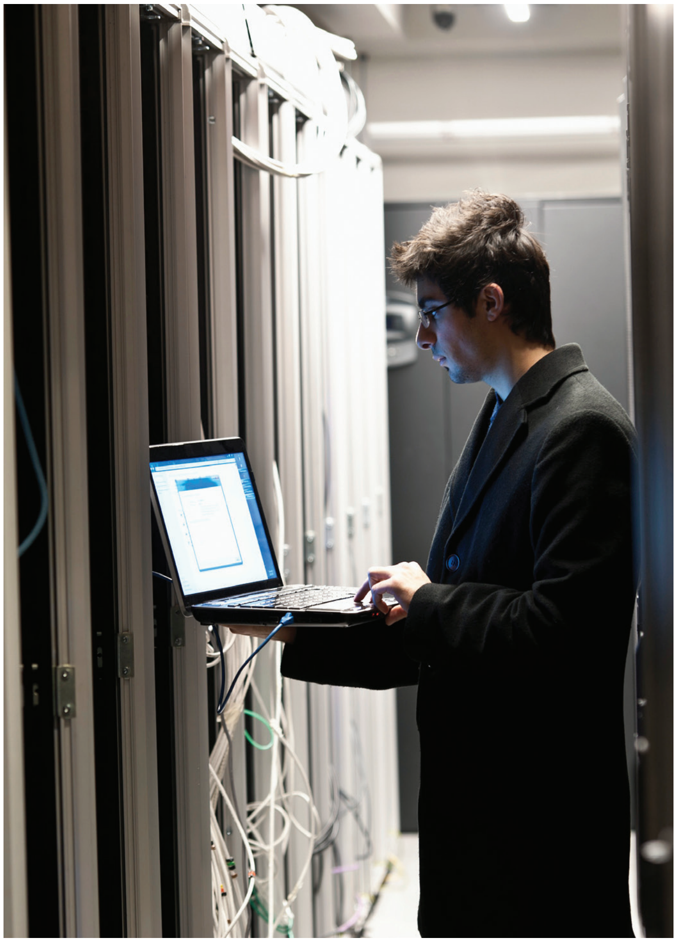
What steps people can take, given the type of information exposed, including the appropriate contact information. For example, this might include contacting the credit reporting agencies to place fraud alerts and credit freezes on their credit files.

If you don't have contact information for all of the affected individuals, you can send press releases or use other means to contact the media and post information to your website.

AFTER RECOVERING FROM A CYBER INCIDENT

Continue monitoring the network for any unusual activity to make sure the intruder has been expelled and you have regained control of your network.

Conduct a post-incident review to identify deficiencies in the planning and execution of your incident response plan.



CYBER INSURANCE

WHAT IS CYBER INSURANCE AND WHY DO I NEED IT?

The costs from a data breach can be very steep and may include lost business, forensic investigations, customer notification expenses, data asset losses and costs to address lawsuits or extortion attempts.

While most businesses have general liability insurance policies, these typically only cover damage to *tangible* property, which does not include electronic data. In fact, even a provision for "digital data protection" may only cover the loss of data due to physical damage.

Cyber insurance can help protect you financially in the event of a cyber attack and should especially be considered if your organization processes payments online, uses cloud systems to store company information, or stores customer data in a computer system.

Talk with your insurance provider about the kind of cyber insurance policy that would best suit your organization.

WHAT SHOULD A CYBER POLICY INCLUDE?

A cyber insurance policy should cover:

- Data breaches (such as incidents involving theft of personal information)
- Cyber attacks (such as breaches of your network)
- Cyber attacks on your data held by vendors and other third parties
- Cyber attacks that occur anywhere in the world (not only in the United States)
- Terrorist acts

Also, consider whether your cyber insurance provider will:

- Defend you in a lawsuit or regulatory investigation (look for "duty to defend" wording)
- Provide coverage in excess of any other applicable insurance you have
- Offer a breach hotline that's available every day of the year at all times

TYPES OF CYBER POLICIES

✓ First-Party Coverage

Protects your data, employee information and customer information. Coverage typically includes costs related to:

- ✔ Legal counsel to determine your notification and regulatory obligations
- ✔ Customer notification and call center services
- ✔ Crisis management and public relations
- ✔ Forensic services to investigate the breach
- ✔ Recovery and replacement of lost or stolen data
- ✔ Lost income due to business interruption
- ✔ Cyber extortion and fraud
- ✔ Fees, fines, and penalties related to the cyber incident

✓ Third-Party Coverage

Generally protects you from liability if a third party brings claims against you. Coverage typically includes:

- ✔ Payments to consumers affected by the breach
- ✔ Claims and settlement expenses related to disputes or lawsuits
- ✔ Losses related to defamation and copyright or trademark infringement
- ✔ Costs for litigation and responding to regulatory inquiries
- ✔ Other settlements, damages, and judgments
- ✔ Accounting costs

APPENDIX How to Securely Wipe Devices Clean before Disposal

✓ COMPUTERS

Before disposing of computers, make sure you securely erase or destroy the hard drive since simply deleting files or formatting the hard drive is not enough to prevent someone from recovering data using easy-to-come-by data recovery software.

First, back up any data you need to a new computer, external drive or web service.

Next, securely erase the hard drive:

PCs

- Use special wiping software to permanently erase your hard drive.
- If, after erasing your drive, you want to take extra precautions, you can physically wipe the drive by dismantling it with a screwdriver, taking a hammer to it or drilling a hole in it.

Macs

- Open Disk Utility from the macOS Utilities window or the Utilities folder of your Applications folder.
- Choose View > Show All Devices.
- Select erase disk, which also erases all volumes on that disk.
- Click the Security Options button. The Security Options window includes a slider that enables you to determine how thoroughly you want to erase your hard drive. There are four notches to that Security Options slider. "Fastest" is quick but insecure — data could potentially be rebuilt using a file recovery app. Moving the slider to the right introduces progressively more secure erasing. Disk Utility's most secure level erases the information used to access the files on your disk, then writes zeroes across the disk surface seven times to help remove any trace of what was there. *NOTE: The more secure method you select, the longer it will take to erase. The most secure methods can take hours.*
- Click Erase, then complete these fields:

  Name: Enter a name for the disk or volume, such as "Macintosh HD".

  Format: Choose either APFS or Mac OS Extended (Journaled) to format as a Mac volume. Disk Utility shows a compatible format by default.

  Scheme (if shown): Choose GUID Partition Map.
- Click Erase.
- Quit Disk Utility when done. You can now install macOS on the disk or volume if you want your Mac to be able to start up from it.
- If, after erasing your drive, you want to take extra precautions, you can physically wipe the drive by dismantling it with a screwdriver, taking a hammer to it or drilling a hole in it.

✓ SMARTPHONES

- Back up all data and contacts.
- Remove external storage such as the SIM card and microSD card.
- Unpair devices.
- Deregister your phone from your accounts. Sign out of email, Find My iPhone and social media apps, then clear the data from these apps. Sign out of/remove iCloud, Google and Samsung accounts.
- Verify that your device is encrypted to prevent someone from restoring any deleted files.

  iPhones since the 3GS are encrypted by default.

  For Android devices, go to Settings > Security and look for an "Encryption" setting. If it says your phone is encrypted, you're all set. If not, tap "Encrypt Phone." The encryption process may take a few hours.

  If your Android phone is older and does not have an encryption option, you can do a factory reset, then use a secure erase app to erase the free space on the phone, and then perform another factory reset.
- Erase your device by doing a factory reset.

  For iPhones, go to Settings > General > Reset and tap "Erase All Content and Settings."

  For most Android phones, go to Settings > System > Reset > "Erase All Data (Factory Reset)."

✓ COPIERS AND FAX MACHINES

Modern copiers and some fax machines contain a hard drive that stores a digital image of every document scanned or copied. So if you have ever copied anything containing confidential information, Social Security numbers, credit card information, or other sensitive or personal identifying information, you need to take measures to ensure it stays out of the hands of identity thieves.

Most manufacturers provide exact instructions on how to clear this data, so check your machine's manual at the time of purchase and before you get rid of it.

If you cannot locate the instructions, follow these steps:

- Install encryption software or disk overwrite software on your copier. Such security software may be preinstalled on new copiers, or you can purchase it separately.
- Perform a disk overwrite before sending the hard drive for service or before returning the hard drive to the copier vendor for disposal.
- Request a signed "certificate of destruction" with the hard drive's model and serial numbers before the vendor removes the copier from the premises.

For additional media sanitization guidelines, see the NIST Special Publication 800-88 at:
https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final

BIBLIOGRAPHY

Bauer, Roderick. (2019, May 19). Getting Rid of Your Mac? Here's How to Securely Erase a Hard Drive or SSD. [Blog post]. Retrieved from www.backblaze.com/blog/how-to-wipe-a-mac-hard-drive/

California Department of Justice, California Chamber of Commerce and Lookout. (2014). *Cybersecurity in the Golden State: How California Businesses Can Protect Against and Respond to Malware, Data Breaches and Other Cyberincidents*. Retrieved from www.oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/2014_cybersecurity_guide.pdf

Data Breach Requirements in Georgia: State Laws. Retrieved from www.techinsurance.com/resources/customer-education/data-breach-laws/georgia/

Federal Trade Commission. (2019). *Data Breach Response: A Guide for Business*. Retrieved from www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business-042519-508.pdf

Federal Trade Commission. (2016). *Protecting Personal Information: A Guide for Business*. Retrieved from www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

Federal Trade Commission, U.S. Department of Commerce-National Institute of Standards of Technology, Small Business Administration, Homeland Security. (2018). *Cybersecurity for Small Business*.

Gordon, Whitson. (2018, May 1). How to Sell Your Old Phone Safely. *New York Times*. Retrieved from www.nytimes.com/2018/05/01/smarter-living/how-to-sell-your-phone-safely.html

How to Manage Your Social Media Privacy Settings. Retrieved from https://identity.utexas.edu/everyone/how-to-manage-your-social-media-privacy-settings

IBM, IBM Security. (2019). *X-Force Threat Intelligence Index 2019*. Retrieved from www.ibm.com/security/data-breach/threat-intelligence

Jungle Disk. (2019, February 11). Does Your Small Business Need Cyber Insurance? Retrieved from www.jungledisk.com/blog/2019/02/11/does-your-small-business-need-cyber-insurance/

Kissel, Regenscheid, Scholl, and Stine. (2014). *Guidelines for Media Sanitization*, (NIST Special Publication 800-88, Revision 1). Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

Koulopoulos, Thomas. (2017, May 11). 60 Percent of Companies Fail in 6 Months Because of This (It's Not What You Think). *Inc*. Retrieved from www.inc.com/thomas-koulopoulos/the-biggest-risk-to-your-business-cant-be-eliminated-heres-how-you-can-survive-i.html

Mansfield, Matt. (2018, December 31.) Cyber Security Statistics: Numbers Small Businesses Need to Know. Retrieved from https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html

Miller, Lucas. (2018, September 24). Why you should(n't) get cyber insurance. Retrieved from https://thenextweb.com/problem-solvers/2018/09/24/why-you-shouldnt-get-cyber-insurance/

Nadeau, Angela. (2018, October 16). 8 Cybersecurity Tips for Your Small Business. Retrieved from https://smallbiztrends.com/2018/10/cybersecurity-tips-for-your-small-business.html

National CyberSecurity Alliance. Small Business Cybersecurity "Quick Wins". Retrieved from https://staysafeonline.org/resource/small-business-quick-wins/

National CyberSecurity Alliance and the Better Business Bureau. Digital Spring Cleaning Checklist for SMBs. Retrieved from https://staysafeonline.org/cybersecure-business/digital-spring-cleaning-checklist-smbs/

Office of the Ohio Attorney General. *Data Breach Prevention and Response Guide for Businesses*. Retrieved from www.ohioattorneygeneral.gov/Files/Publications-Files/Publications-for-Business/Data-Breach-Prevention-and-Response-Guide-for-Smal

Ponemon Institute. (2018). *2018 State of Cybersecurity in Small & Medium Size Businesses (SMB)*. Retrieved from https://keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf

Ponemon Institute. (2019). *The Cyber Resilient Organization*. Retrieved from www.ibm.com/account/reg/us-en/signup?formid=urx-37792

Protect Against Ransomware. Retrieved from www.sba.gov/managing-business/cybersecurity/protect-against-ransomware

Small Business Computer Security Basics. Retrieved from www.ftc.gov/tips-advice/business-center/guidance/small-business-computer-security-basics

Stockton, Gary. (2018, November 28). Why your small business needs cybersecurity. Retrieved from www.experian.com/blogs/small-business-matters/2018/11/28/why-your-small-business-needs-cybersecurity/

U.S. Department of Justice, Criminal Division, Computer Crime & Intellectual Property Section, Cybersecurity Unit. (2018). *Best Practices for Victim Response and Reporting of Cyber Incidents (Version 2.0)*. Retrieved from www.justice.gov/criminal-ccips/file/1096971/download

Verizon. (2018). *2018 Data Breach Investigations Report*. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/

(internet network
p2p

GEORGIA DEPARTMENT OF LAW
CONSUMER PROTECTION DIVISION

2 Martin Luther King, Jr. Drive
Suite 356 - East Tower
Atlanta, Georgia 30334

404-458-3800

consumer.ga.gov