Session Description:

Every day the news is filled with the latest ransomware attack, mass identity theft, data breach, and zero-day attack. Even so, a majority of businesses remain unsure how to best prepare for a cyber incident, whom they can turn to for practical and informed help, or when and where to start. Even companies that have a plan are missing opportunities to better align their security strategies, mature their cyber defenses, and shore up their weakest links (usually your employees who, in the press of business demands and pressures, don’t internalize the fact that sometimes the entire organization is literally just one click away from a devastating cyber breach). Yet others still don’t even have an incident response plan at all.

Regulators are increasingly issuing cybersecurity mandates while at the same time, organizations continue to navigate constant changes that increase their cyber risk profile. As was once said: there are two types of companies – those who have been hacked, and those who have but don’t know it yet. In short, no organization, regardless of industry or size, can afford to keep their head in the sand.

Join us for a practical discussion where we’ll walk through the basics of cybersecurity best practices, how to efficiently identify and prioritize your highest cyber risks and leverage your existing governance and compliance structures, and how to create or enhance your cyber incident response and insider threat plans.

Moderator:
Angeline G. Chen, Of Counsel, DLA Piper

Speakers:
Shaila Lakhani Ohri, Assistant General Counsel, Exelon
Scott Takaoka, Senior Director, Imperium Consulting Group
Manning the Gates
How to Prepare Your Company for a Cyber Breach
Speakers

• Shaila Lakhani Ohri, Assistant General Counsel, Exelon
• Scott Takaoka, Senior Director, Imperium Consulting Group

Moderator/Speaker

• Angeline G. Chen, Of Counsel, DLA Piper
Agenda

- What is a Cyber Breach Anyway?
- The Current Cyber Landscape
- Legal and Regulatory Considerations
- Developing Your Incident Response Plan and Strategy
- How Much Is Enough
What is a Cyber Breach Anyway?
Setting our Baseline

A “cyber breach” versus a “cyber incident”

• Terms can sometimes be interchangeable
• Distinctions can be:
  • Situational
  • Regulatory
  • Contractual
  • Set by governance frameworks or standards, or
  • Industry/market driven
• Degree of severity (of expected or actual impact)
Definition

[Legal boilerplate language: *For purposes of this presentation ...*]

A cyber breach is an incident through which:

- confidential, sensitive, or protected information is disclosed, stolen, or taken from an information system:
  - without the knowledge or authorization of the system’s (or the data’s) owner, and/or
  - to or by an unauthorized person, and/or
- Unauthorized access to an organization’s electronic digitized data, applications, networks or devices that is achieved by an intentional actor.
The Current Cyber Landscape
Recent Security Breaches

Details murky in Samsung’s second data breach this year
By Aaron Nicodemus | Tue, Sep 6, 2022 5:49 PM

South Korean electronics giant announced it discovered a second data breach in 2022, with details about the incident remaining unclear.

Apple, Meta, and Discord Address Reports Of Being Tricked Into Giving User Data to Hackers

Hackers sent fraudulent data requests to both tech companies.

Updated: Mar 31, 2022 5:07 pm

DoorDash Data Breach Exposed Some Personal Customer Data

200k North Face customers lose data in a breach

Vilus Petkauskas, Journalist Updated on: 09 September 2022

Photographer: Gabby Jones/Bloomberg

FishPig software breach puts up to 200,000 websites at risk

SC Staff | September 15, 2022

Ars Technica reports that up to 200,000 websites are at risk of compromise following the breach of e-commerce software provider FishPig’s systems in a supply chain attack that involved the deployment of the sophisticated Rekoobe backdoor malware.
Threat/Attack Vectors

A threat or attack vector is the path or means by which a Threat Actor gains access to an information system to exploit vulnerabilities and carry out an attack.
What are the Threat Actors after?

• **TLDR: EVERYTHING**

**HIGH VALUE DATA**
- Personally Identifiable Information (PII)
  - Social Security Numbers
  - Personal Identifiers
- Intellectual Property / Trade Secrets
- Financial Information
  - Credit card numbers
  - Bank account numbers
- Protected Health Information (PHI)
- Passwords

**LEVERAGE AND EXPLOITATION**
- Financial Gain
- Business Disruption
- Corporate Espionage
- Sabotage/Vandalism/Nuisance
- Hacker/group reputation (notoriety)
- Organized Crime
- Blackmail/Extortion
- Advanced Persistent Threat
- Curiosity/Boredom

IT’S NOT A MATTER OF “IF” BUT “WHEN”.

#NAPABA22
# How do They Get Past the Gate?

<table>
<thead>
<tr>
<th>MITRE ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA0001</td>
<td>Initial Access</td>
<td>To enter the system</td>
</tr>
<tr>
<td>TA0002</td>
<td>Execution</td>
<td>To run malicious code</td>
</tr>
<tr>
<td>TA0003</td>
<td>Persistence</td>
<td>To maintain a foothold</td>
</tr>
<tr>
<td>TA0004</td>
<td>Privilege Escalation</td>
<td>To gain higher-level permissions</td>
</tr>
<tr>
<td>TA0005</td>
<td>Defence Evasion</td>
<td>To avoid being detected</td>
</tr>
<tr>
<td>TA0006</td>
<td>Credential Access</td>
<td>To steal account names and passwords</td>
</tr>
<tr>
<td>TA0007</td>
<td>Discovery</td>
<td>To learn about the system environment</td>
</tr>
<tr>
<td>TA0008</td>
<td>Lateral Movement</td>
<td>To move throughout the system environment</td>
</tr>
<tr>
<td>TA0009</td>
<td>Collection</td>
<td>To gather information of interest</td>
</tr>
<tr>
<td>TA0011</td>
<td>Command and Control</td>
<td>To control a compromised system</td>
</tr>
<tr>
<td>TA0010</td>
<td>Exfiltration</td>
<td>To steal data</td>
</tr>
<tr>
<td>TA0040</td>
<td>Impact</td>
<td>To manipulate, interrupt, or destroy your system and data</td>
</tr>
</tbody>
</table>

MITRE ATT&CK Categories of Tactics. Attack matrices can be found at https://attack.mitre.org.
The process by which cyber attacks are executed can be represented as a "life cycle."
Cyber Attack Trends

*Ransomware and data breach are now one

- 2018 – Year of the large data breach
  - Facebook 87M records
  - Under Armour 150M records
  - Marriott 500M records
- 2019 tactics transition to ransomware

<table>
<thead>
<tr>
<th>Year</th>
<th>Ransom</th>
<th>Downtime</th>
<th>Data Exfiltration</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019*</td>
<td>$84k</td>
<td>16 days</td>
<td>5%</td>
</tr>
<tr>
<td>2020</td>
<td>$154k</td>
<td>21 days</td>
<td>70%</td>
</tr>
<tr>
<td>2021</td>
<td>$322k</td>
<td>20 days</td>
<td>84%</td>
</tr>
<tr>
<td>Q1 2022</td>
<td>$211k</td>
<td>26 days</td>
<td>77%</td>
</tr>
</tbody>
</table>

**Data Breach vs. Ransomware**

- Data Breach (Confidentiality)
- Ransomware (Availability)

*Coveware blogs – January 23, 2020 – May 3, 2022
**Data based on Verizon 2022 DBIR
Ransomware Attack Targeting

- Nearly 1/2 of ransomware attacks take place in mid-market companies between 1,000 and 10,000 employees.
- Mid-market companies typically have lower cyber security maturity.
- Large enterprise are not immune – software vulnerability attacks (log4j, Kaseya, Fortinet) leave them exposed.
Impact of Cyber Incidents

• The average data breach cost in 2022 was $4.35 million
• This is an increase of 2.6% year-over-year from 2021
• The breach costs increased the most between 2020 and 2021, likely due to the COVID-19 pandemic
• Organizations working from remote paid an average of almost $1 million more than organizations that did not utilize a remote working model
• Healthcare had the highest data breach costs of any industry for the twelfth consecutive year (paying an average of $10M for a data breach

Source: 2022 Cost of a Data Breach Report by IBM and The Ponemon Institute
Legal and Regulatory Considerations
For the Record ...

What is the difference between cybersecurity and privacy?

- CYBERSECURITY: Safeguarding the data, the systems, and the people (including but not limited to protecting against the unauthorized access to data)

- PRIVACY: Safeguarding user identify

Distinguishing between these two domains can be complex, and there are certainly areas of overlap between the two.
Partial List of Relevant Laws and Requirements

- Sarbanes-Oxley (Pub L. 107-294)
- General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI DSS)
- Federal Trade Commission Act (15 USC § 41 et seq)
- The Defense Federal Acquisition Regulation Supplement (DFARS)
- International Traffic in Arms Regulations (22 CFR 120-130)
- NIST 800-171 and NIST 800-172 standards
- Children’s Online Privacy Protection Act (15 USC § 6501 et seq)
- State privacy laws
- Cyber Maturity Model Certification (CMMC)

Typical Legal / Regulatory Requirements

- Notification
- Reporting
- Self-Assessments / Third-Party Assessments
- Systems and Access Controls
- Information Security and Assurance Policies and Procedures
- Compliance with Specific Standards
- Provision of Credit Monitoring / other Services to Impacted Individuals
- Training
Incident Responses, Plans, and Strategy
If You’re Scrambling ...

LIMIT
Limit additional damage.
PULL THE PLUG
Filter traffic
Isolate system.

SURVEY
Survey the damage
Identify the attacker.
Discovery the vulnerability.

RECORD
Record and document the event.
Find effects
Identify disruptions.

ENGAGE
Engage with LE.

NOTIFY
Identify affected parties.
Notify affected persons.

LEARN
Document learning points.
Proactively ensure learning.

IMMEDIATELY
• Inform your senior leadership and the board.
• Engage outside counsel to assert and preserve attorney client privilege.
• Assemble a team.

Source in part: Gunpreet Dhillon, What to do before and after a cybersecurity breach (Virginia Commonwealth University, Kogod School of Business 2015.)
Cybersecurity and Breach Program Elements

**IDENTIFY**
- Asset
- Environment
- Governance
- Risks
- Strategies

**PROTECT**
- Access
- Awareness
- Data
- Information
- Maintenance
- Protective tools

**DETECT**
- Anomalies
- Events
- Continuous monitoring
- Detection processes

**RESPOND**
- Response plans
- Comms
- Analysis
- Mitigate
- Improve

**RECOVER**
- Planning
- Improve
- Comms
- CA/CI

#NAPABA22
What does an Incident Response (“IR”) Plan do?

• Provides a roadmap on how to respond to an incident
• Maps potential security risks, impacts and mitigations to relevant industry standards and regulations applicable to your business
• Identifies security response roles and responsibilities across all departments and stakeholders
• Identifies an escalation path for different cyber threats
• Sets forth remediation procedures to respond to incidents in a way that maintains compliance with applicable standards and regulations
• Provides for communication plans to keep stakeholders informed during the incident handing and response processes, engage with government authorities, and notify victims if PII is compromised
Incident Response Plan Phases

- PREPARATION
- IDENTIFICATION / DETECTION & ANALYSIS
- CONTAINMENT
- ERADICATION
- RECOVERY
- LESSONS LEARNED / POST-INCIDENT ACTIVITY

Sources: NIST Computer Security Incident Handling Guide and the SANS Institute.
Roadmap to Developing an IR Plan

• Create a **plan and framework**
• Form and stand up an **incident response team** and define **roles and responsibilities**
• Develop **policies and procedures**
• Create a **communication plan** (and keep it updated!)
• Identify **lessons learned**
• **Proof test**

Sources: NIST Computer Security Incident Handling Guide and the SANS Institute.
Operationalize your Policy

- Discusses integration of security and insurance processes during a cyber event
- Contemplates maintaining attorney client privilege
- Trains client on what to do during an event
- Establishes need for Incident Response services
- Creates bridges with team members and partners
Is an IR Plan mandatory?

• All 50 states and many countries and regions around the world have various breach notification laws that require organizations to notify victims of security preaches where PII is compromised.
• Multiple regulations mandate an IR Plan:
  • Payment Card Industry (PCI) – Rule 12.10
  • HIPAA – Security Rule
  • New York Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR 50)
  • Gramm-Leach Bliley Act
  • Federal Trade Commission
How Much is Enough?
Understanding Risk Management

• Understand your organization’s risk profile and risk tolerance
• Develop a risk management approach
• “Must” Considerations
  • What industry(ies) are you in?
  • What market requirements (e.g., SEC, NYSE) apply?
  • What kind of information do you collect / hold / provide?
• Standards
• Availability and Coverage Afforded by Insurance
Continuous Improvement / Cyber Risk Management Lifecycle

- **Integrates** risk management and security efforts
- **Flows** across the organization
- **Supports** the business
- **Enables** business by managing risk security and risk transfer
Cyber Liability Insurance Trends in 2022

### Increased underwriting rigor
- Carriers are closely scrutinizing cyber security controls
- Clients with poor controls experience:
  - Declinations from incumbent carriers
  - Refusal to quote from new markets
  - Subjectivity resolution no later than binding

### Reduction in coverage terms
- Carriers are limiting their exposure within a client
- Elimination or co-insurance for ransomware loss
- Longer waiting period for business interruption coverage
- Concerns of war exclusion, exposure to Russia and Belarus

### Overall cyber market - aggregate risk
- Aggregate cyber exposure concern – Kaseya, log4...
- Contracting limits, $5M or less
- Contingent business interruption sub-limited or eliminated
- Concerns of war exclusion, exposure to Russia and Belarus
- Exiting some markets - mfg, healthcare, critical infrastructure, public sector

### Higher premiums
- Premium increase of 100% are not uncommon
- Increase in retentions especially in the mid-market
- Increased cost of cyber and decrease in market capacity resulting in reduction in obtained limits in many clients
Maturity Rating and Quantification

• Assess and measure control maturity and quantification
  - understand control impact on potential loss in $s
Resources:

- MITRE ATT&CK knowledge base of adversary tactics and techniques, located at https://attack.mitre.org
- Coveware Ransomware Recovery blog, at https://www.coveware.com/blog
- Verizon 2022 Data Breach Investigation Report
- 2022 Cost of a Data Breach Report by IBM and the Ponemon Institute
- FTC Small Business Cybersecurity Materials
- DLA Piper Data Breach Response Guide
QUESTIONS?
A data breach is any unauthorized acquisition or release of, or access to, information, which usually exposes the information to an untrusted environment. Though legal definitions vary, data breaches come in all shapes and sizes, such as files or documents stolen from an office or car; lost laptops, mobile devices, or tablets; compromised servers or e-mail accounts; hacked computers or social media accounts; and APTs (advanced persistent threats).

Data breaches can cost a company millions of dollars in mitigation and remediation costs (an average of $5.4 million per breach in the U.S. in 2011), and cause significant harm to its brand and reputation. The first 24 hours after you discover a breach are critical to restoring security, minimizing harm, obtaining and preserving evidence, and complying with contractual and legal obligations. This checklist provides company executives and in-house counsel with prioritized key steps to take (and not to take) in response to a breach.

<p>| Assemble an Incident Response Team (IRT) | The makeup of an IRT will depend upon the kind of breach, what information/data was lost, and what the threat vector was. It may include: An executive with decision making authority; A team leader responsible for response coordination, contacting outside counsel and the forensics team, and addressing press inquiries; “First-responder” security and IT personnel with access to systems and permissions; Representatives from key departments, including IT, Legal, Human Resources, Customer Relations, Risk Management, Communications/Public Relations, Operations (for physical breaches), and/or Finance (for breaches involving loss of company financial information); CIO, CISO, CPO, CITO and/or other C-level stakeholders; and Outside counsel. |
| Contact Inside and Outside Counsel to Establish a “Privileged” Reporting/Communication Channel | Establishing a privileged reporting channel (ideally before a breach occurs) maintains the confidentiality of the investigation. Counsel should provide legal advice, retain forensic cyber security experts, and direct response actions every step of the way to protect the confidentiality of the investigation and of applicable internal communications under the attorney-client privilege and work product doctrine. Consider emphasis on use of telephone for critical and sensitive communications in the event that e-mail and electronic communications channels may be compromised. Counsel should also be involved in the establishment of the investigative team and receive all incident reports (initial, draft, and final), including IT-related communications, for the purposes of providing legal advice. Outside counsel can also work (and have established relationships) with law enforcement and forensic experts who can assess risk and provide guidance on remediation, disclosure, and notification efforts. |</p>
<table>
<thead>
<tr>
<th><strong>Coordinate with Legal Counsel to Bring in Cyber Security Experts and Forensic Examiners</strong></th>
</tr>
</thead>
</table>
| In the rush to mitigate a breach, internal security and IT often are not in a position to verify the depth and extent of a breach, especially when an APT (advanced persistent threat) is involved or the hackers have left “backdoors” to permit subsequent access. Forensic experts, retained and directed by legal counsel, bring independence to investigations, and are free from real or perceived conflicts that might be imputed to internal IT and security personnel who manage the affected systems. Further, by retaining experts via legal counsel, communications prepared for or by the experts can be protected by the attorney-client privilege.  

Through counsel, forensic experts can advise your organization how to proceed to stop data loss, secure evidence, and prevent further harm. They are also trained to preserve ephemeral evidence and manage the chain of custody, minimizing the chance that evidence will be altered, destroyed, or rendered inadmissible in court. |

<table>
<thead>
<tr>
<th><strong>Stop Additional Data Loss</strong></th>
</tr>
</thead>
</table>
| If the breach is ongoing, consult with forensic experts, trained IT staff, and security personnel about taking affected systems offline by disconnecting them from the network and/or using tools to dynamically image affected systems to preserve evidence.  

If paper records or other physical assets were compromised obtain tracking information, logs, and surveillance evidence, if available. |

<table>
<thead>
<tr>
<th><strong>Secure Evidence</strong></th>
</tr>
</thead>
</table>
| Secure and prevent physical access to affected systems, such as servers and workstations, to maintain the integrity of the evidence and ensure that only selected forensic experts and law enforcement (if applicable) have access. Preserve all security access device (token, key card, building credentials, etc.) logs and surveillance tapes. Work with counsel to send preservation letters to service and cloud providers. Track the chain of custody (i.e., who had contact with the affected system, what did they do, and who was the next to touch the affected system) for all physical or digital evidence. Inventory any missing hardware.  

If the compromise occurred on vendor’s computer systems, or was the result of a vendor’s loss of paper, media, or data in other traditional physical forms, request retention and copies of relevant evidence, such as forensic server images, logs, tracking information, video surveillance, and e-mail. |

<table>
<thead>
<tr>
<th><strong>Preserve Computer Logs</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Preserve all affected system log files, including firewall, VPN, mail, network, client, web, server, and intrusion detection system logs. These logs are critical to assessing the origins of the attack, its duration, and volume of data exfiltrated during the breach.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Document the Breach</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Record the date and time of the breach, the personnel who discovered the breach, the nature of the breach, the kinds of data stolen/lost, when the response efforts began, and all of the employees who had access to the affected systems. Document all data and/or devices and hardware lost in the breach. Because a high percentage of data breaches can be traced to former employees, obtain names and contact information for all employees terminated within the last 90-120 days, and confirm that their security access has been terminated.</td>
</tr>
</tbody>
</table>
### Contact Law Enforcement (Possibly)

After consultation with legal counsel and upper management, determine whether contacting law enforcement is necessary (especially where E.U. “data subjects” are involved), prudent, and/or valuable. In some cases, but not all, you may be able to delay notification requirements if it would impede or interfere with a law enforcement investigation. Law enforcement’s expertise in evidence gathering and forensics can be leveraged to ensure that the evidence can be used in future court proceedings.

### Define Legal Obligations

Domestic breach notification laws vary from state to state. In addition, your organization may have notification obligations under other the law of other countries if data for non-U.S. individuals was lost. Legal requirements will also vary depending on the types of data, the venues at issue, and the form in which the data is stored. Among other things, these laws affect the timing, content, and form of any required notification. With guidance from counsel, determine whether there are also obligations to notify service providers, payment card networks, or other contractual partners.

Additionally, engage counsel to review insurance policies to determine whether insurance carriers should be notified to preserve coverage rights.

### Conduct Interviews of Personnel Involved

Identify all of the individuals who were involved in the discovery and initial investigation of the breach. Conduct interviews to create a complete record of all efforts taken to stop data loss, secure systems, mitigate damage and harm, etc. Determine whether counsel (inside or outside) should participate in the interviews and be present if law enforcement also requests interviews with relevant personnel.

### Reissue or Force Security Access Changes

Increasingly, cyber criminals are after log-in credential and password combinations. After a breach, personnel should be required to change passwords and be issued new physical authentication/access devices (tokens, badges, key cards, etc.). Because intruders are often after the personally identifying information of employees, as well as customers, these same personnel should also be strongly encouraged to change passwords for their personal banking, healthcare, web mail, and social media accounts/passwords.

### Do Not Probe Computers and Affected Systems

Evidence could be accidentally altered or lost, or intruders could be alerted to your activities, causing them to take measures to hide their trail, damaging your systems in the process.

### Do Not Turn Off Computers and Affected Systems

Valuable information can be stored in temporary memory storage spaces that could be lost if you unnecessarily turn off a running system. If an affected system is on and/or connected, leave it on and connected. Work with forensic experts to determine whether the system should be dynamically imaged before disconnecting it to avoid tipping cyber criminals to the fact that you are aware of the breach and to preserve evidence that they might otherwise destroy to conceal their tracks. If the system is off, unplug it.
Do Not Image or Copy Data, or Connect Storage Devices/Media, to Affected Systems

Imaging and copying of affected systems should be left to forensic experts and law enforcement agents who are equipped with state-of-the-art forensic toolkits and imaging utilities. Copying data without the right protocols and tools (even for the purpose of providing to law enforcement) can alter or destroy important evidence, and render evidence inadmissible in court.

Do Not Run Antivirus Programs or Utilities

Running programs or utilities on the affected systems could result in the accidental loss or destruction of evidence.

Do Not Reconnect Affected Systems

Affected systems should be preserved until forensic or law enforcement examination and remediation efforts have been completed. A “cleaned” system is not always clean. Backdoors and persistent threats are designed to lull personnel into a false sense of security. All affected systems should go through rigorous testing and verification before being reconnected to the network.

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help clients with their legal needs around the world.

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:

Andrew Serwin
Partner
US Chair and Global Co-Chair, Data Protection, Privacy and Security Practice
US Chair and Global Co-Chair, Cybersecurity Practice
T +1 858 677 1418
andrew.serwin@dlapiper.com

Angeline Chen
Of Counsel
T +1 202 799 4107
angeline.chen@dlapiper.com
CYBERSECURITY BASICS

Cyber criminals target companies of all sizes. Knowing some cybersecurity basics and putting them in practice will help you protect your business and reduce the risk of a cyber attack.

PROTECT YOUR FILES & DEVICES

Update your software
This includes your apps, web browsers, and operating systems. Set updates to happen automatically.

Secure your files
Back up important files offline, on an external hard drive, or in the cloud. Make sure you store your paper files securely, too.

Require passwords
Use passwords for all laptops, tablets, and smartphones. Don’t leave these devices unattended in public places.

Encrypt devices
Encrypt devices and other media that contain sensitive personal information. This includes laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage solutions.

Use multi-factor authentication
Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that’s inserted into a computer.

LEARN MORE AT: FTC.gov/SmallBusiness
CYBERSECURITY FOR SMALL BUSINESS

PROTECT YOUR WIRELESS NETWORK

Secure your router
Change the default name and password, turn off remote management, and log out as the administrator once the router is set up.

Use at least WPA2 encryption
Make sure your router offers WPA2 or WPA3 encryption, and that it’s turned on. Encryption protects information sent over your network so it can’t be read by outsiders.

MAKE SMART SECURITY YOUR BUSINESS AS USUAL

Require strong passwords
A strong password is at least 12 characters that are a mix of numbers, symbols, and capital lowercase letters.

Never reuse passwords and don’t share them on the phone, in texts, or by email.

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

Train all staff
Create a culture of security by implementing a regular schedule of employee training.

Update employees as you find out about new risks and vulnerabilities. If employees don’t attend, consider blocking their access to the network.

Have a plan
Have a plan for saving data, running the business, and notifying customers if you experience a breach. The FTC’s Data Breach Response: A Guide for Business gives steps you can take. You can find it at FTC.gov/DataBreach.

LEARN MORE AT: FTC.gov/SmallBusiness
Understanding THE NIST CYBERSECURITY FRAMEWORK

You may have heard about the NIST Cybersecurity Framework, but what exactly is it?

And does it apply to you?

NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The Framework is voluntary. It gives your business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection.

You can put the NIST Cybersecurity Framework to work in your business in these five areas: Identify, Protect, Detect, Respond, and Recover.

1. **IDENTIFY**

   Make a list of all equipment, software, and data you use, including laptops, smartphones, tablets, and point-of-sale devices.

   Create and share a company cybersecurity policy that covers:

   - Roles and responsibilities for employees, vendors, and anyone else with access to sensitive data.
   - Steps to take to protect against an attack and limit the damage if one occurs.

2. **PROTECT**

   - Control who logs on to your network and uses your computers and other devices.
   - Use security software to protect data.
   - Encrypt sensitive data, at rest and in transit.
   - Conduct regular backups of data.
   - Update security software regularly, automating those updates if possible.
   - Have formal policies for safely disposing of electronic files and old devices.
   - Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.
3. DETECT

- Monitor your computers for unauthorized personnel access, devices (like USB drives), and software.
- Check your network for unauthorized users or connections.
- Investigate any unusual activities on your network or by your staff.

4. Respond

Have a plan for:

- Notifying customers, employees, and others whose data may be at risk.
- Keeping business operations up and running.
- Reporting the attack to law enforcement and other authorities.
- Investigating and containing an attack.
- Updating your cybersecurity policy and plan with lessons learned.
- Preparing for inadvertent events (like weather emergencies) that may put data at risk.
- Test your plan regularly.

5. Recover

After an attack:

- Repair and restore the equipment and parts of your network that were affected.
- Keep employees and customers informed of your response and recovery activities.

For more information on the NIST Cybersecurity Framework and resources for small businesses, go to NIST.gov/CyberFramework and NIST.gov/Programs-Projects/Small-Business-Corner-SBC.
PHYSICAL SECURITY

Cybersecurity begins with strong physical security.

Lapses in physical security can expose sensitive company data to identity theft, with potentially serious consequences. For example:

An employee accidentally leaves a flash drive on a coffeehouse table. When he returns hours later to get it, the drive — with hundreds of Social Security numbers saved on it — is gone.

Another employee throws stacks of old company bank records into a trash can, where a criminal finds them after business hours.

A burglar steals files and computers from your office after entering through an unlocked window.

HOW TO PROTECT EQUIPMENT & PAPER FILES

Here are some tips for protecting information in paper files and on hard drives, flash drives, laptops, point-of-sale devices, and other equipment.

**Store securely**
When paper files or electronic devices contain sensitive information, store them in a locked cabinet or room.

**Limit physical access**
When records or devices contain sensitive data, allow access only to those who need it.

**Send reminders**
Remind employees to put paper files in locked file cabinets, log out of your network and applications, and never leave files or devices with sensitive data unattended.

**Keep stock**
Keep track of and secure any devices that collect sensitive customer information. Only keep files and data you need and know who has access to them.

LEARN MORE AT: FTC.gov/SmallBusiness
HOW TO PROTECT DATA ON YOUR DEVICES

A burglary, lost laptop, stolen mobile phone, or misplaced flash drive — all can happen due to lapses in physical security. But they’re less likely to result in a data breach if information on those devices is protected. Here are a few ways to do that:

Require complex passwords
Require passwords that are long, complex, and unique. And make sure that these passwords are stored securely. Consider using a password manager.

Use multi-factor authentication
Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.

Limit login attempts
Limit the number of incorrect login attempts allowed to unlock devices. This will help protect against intruders.

Encrypt
Encrypt portable media, including laptops and thumb drives, that contain sensitive information. Encrypt any sensitive data you send outside of the company, like to an accountant or a shipping service.

TRAIN YOUR EMPLOYEES
Include physical security in your regular employee trainings and communications. Remind employees to:

Shred documents
Always shred documents with sensitive information before throwing them away.

Erase data correctly
Use software to erase data before donating or discarding old computers, mobile devices, digital copiers, and drives. Don’t rely on “delete” alone. That does not actually remove the file from the computer.

Promote security practices in all locations
Maintain security practices even if working remotely from home or on business travel.

Know the response plan
All staff should know what to do if equipment or paper files are lost or stolen, including whom to notify and what to do next. Use Data Breach Response: A Guide for Business for help creating a response plan. You can find it at FTC.gov/DataBreach.

LEARN MORE AT:
FTC.gov/SmallBusiness
RANSOMWARE

Someone in your company gets an email.

It looks legitimate — but with one click on a link, or one download of an attachment, everyone is locked out of your network. That link downloaded software that holds your data hostage. That’s a ransomware attack.

The attackers ask for money or cryptocurrency, but even if you pay, you don’t know if the cybercriminals will keep your data or destroy your files. Meanwhile, the information you need to run your business and sensitive details about your customers, employees, and company are now in criminal hands. Ransomware can take a serious toll on your business.

HOW IT HAPPENS

Criminals can start a ransomware attack in a variety of ways.

**Scam emails**
with links and attachments that put your data and network at risk. These phishing emails make up most ransomware attacks.

**Server vulnerabilities**
which can be exploited by hackers.

**Infected websites**
that automatically download malicious software onto your computer.

**Online ads**
that contain malicious code — even on websites you know and trust.
HOW TO PROTECT YOUR BUSINESS

Have a plan
How would your business stay up and running after a ransomware attack? Put this plan in writing and share it with everyone who needs to know.

Back up your data
Regularly save important files to a drive or server that’s not connected to your network. Make data backup part of your routine business operations.

Keep your security up to date
Always install the latest patches and updates. Look for additional means of protection, like email authentication, and intrusion prevention software, and set them to update automatically on your computer. On mobile devices, you may have to do it manually.

Alert your staff
Teach them how to avoid phishing scams and show them some of the common ways computers and devices become infected. Include tips for spotting and protecting against ransomware in your regular orientation and training.

WHAT TO DO IF YOU’RE ATTACKED

Limit the damage
Immediately disconnect the infected computers or devices from your network. If your data has been stolen, take steps to protect your company and notify those who might be affected.

Contact the authorities
Report the attack right away to your local FBI office.

Notify customers
If your data or personal information was compromised, make sure you notify the affected parties – they could be at risk of identity theft. Find information on how to do that at Data Breach Response: A Guide for Business. You can find it at FTC.gov/DataBreach.

Keep your business running
Now’s the time to implement that plan. Having data backed up will help.

Should I pay the ransom?
Law enforcement doesn’t recommend that, but it’s up to you to determine whether the risks and costs of paying are worth the possibility of getting your files back. However, paying the ransom may not guarantee you get your data back.

LEARN MORE AT:
FTC.gov/SmallBusiness
You get an email that looks like it’s from someone you know.

It seems to be from one of your company’s vendors and asks that you click on a link to update your business account. Should you click? Maybe it looks like it’s from your boss and asks for your network password. Should you reply? In either case, probably not. These may be phishing attempts.

**HOW PHISHING WORKS**

**You get an email or text**

It seems to be from someone you know, and it asks you to click a link, or give your password, business bank account, or other sensitive information.

**It looks real**

It’s easy to spoof logos and make up fake email addresses. Scammers use familiar company names or pretend to be someone you know.

**It’s urgent**

The message pressures you to act now — or something bad will happen.

**What happens next**

If you click on a link, scammers can install ransomware or other programs that can lock you out of your data and spread to the entire company network. If you share passwords, scammers now have access to all those accounts.

**WHAT YOU CAN DO**

**Before you click on a link or share any of your sensitive business information:**

**Check it out**

Look up the website or phone number for the company or person behind the text or email. Make sure that you’re getting the real company and not about to download malware or talk to a scammer.

**Talk to someone**

Talking to a colleague might help you figure out if the request is real or a phishing attempt.

**Make a call if you’re not sure**

Pick up the phone and call that vendor, colleague, or client who sent the email. Confirm that they really need information from you. Use a number you know to be correct, not the number in the email or text.
**CYBERSECURITY FOR SMALL BUSINESS**

**HOW TO PROTECT YOUR BUSINESS**

**Back up your data**
Regularly back up your data and make sure those backups are not connected to the network. That way, if a phishing attack happens and hackers get to your network, you can restore your data. Make data backup part of your routine business operations.

**Keep your security up to date**
Always install the latest patches and updates. Look for additional means of protection, like email authentication and intrusion prevention software, and set them to update automatically on your computers. On mobile devices, you may have to do it manually.

**Alert your staff**
Share with them this information. Keep in mind that phishing scammers change their tactics often, so make sure you include tips for spotting the latest phishing schemes in your regular training.

**Deploy a safety net**
Use email authentication technology to help prevent phishing emails from reaching your company’s inboxes in the first place.

**WHAT IF YOU FALL FOR A PHISHING SCHEME**

**Alert others**
Talk to your colleagues and share your experience. Phishing attacks often happen to more than one person in a company.

**Limit the damage**
Immediately change any compromised passwords and disconnect from the network any computer or device that’s infected with malware.

**Follow your company’s procedures**
These may include notifying specific people in your organization or contractors that help you with IT.

**Notify customers**
If your data or personal information was compromised, make sure you notify the affected parties — they could be at risk of identity theft. Find information on how to do that at Data Breach Response: A Guide for Business (FTC.gov/DataBreach).

**Report it**
Forward phishing emails to spam@uce.gov (an address used by the FTC) and to reportphishing@apwg.org (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies). Let the company or person that was impersonated know about the phishing scheme. And report it to the FTC at FTC.gov/Complaint.

**LEARN MORE AT:**
FTC.gov/SmallBusiness
A scammer sets up an email address that looks like it’s from your company. Then the scammer sends out messages using that email address. This practice is called spoofing, and the scammer is what we call a business email imposter. Scammers do this to get passwords and bank account numbers or to get someone to send them money. When this happens, your company has a lot to lose. Customers and partners might lose trust and take their business elsewhere — and your business could then lose money.

**How to Protect Your Business**

**Use email authentication**
When you set up your business's email, make sure the email provider offers email authentication technology. That way, when you send an email from your company’s server, the receiving servers can confirm that the email is really from you. If it’s not, the receiving servers may block the email and foil a business email imposter.

**Keep your security up to date**
Always install the latest patches and updates. Set them to update automatically on your network. Look for additional means of protection, like intrusion prevention software, which checks your network for suspicious activity and sends you alerts if it finds any.

**Train your staff**
Teach them how to avoid phishing scams and show them some of the common ways attackers can infect computers and devices with malware. Include tips for spotting and protecting against cyber threats in your regular employee trainings and communications.

**Learn More At:**
FTC.gov/SmallBusiness
WHAT TO DO
IF SOMEONE SPOOFS YOUR COMPANY’S EMAIL

Report it
Report the scam to local law enforcement, the FBI’s Internet Crime Complaint Center at IC3.gov, and the FTC at FTC.gov/Complaint. You can also forward phishing emails to spam@uce.gov (an address used by the FTC) and to reportphishing@apwg.org (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies).

Notify your customers
If you find out scammers are impersonating your business, tell your customers as soon as possible — by mail, email, or social media. If you email your customers, send an email without hyperlinks. You don’t want your notification email to look like a phishing scam. Remind customers not to share any personal information through email or text. If your customers’ data was stolen, direct them to IdentityTheft.gov to get a recovery plan.

Alert your staff
Use this experience to update your security practices and train your staff about cyber threats.

LEARN MORE AT:
FTC.gov/SmallBusiness
You get a phone call, pop-up, or email telling you there’s a problem with your computer. Often, scammers are behind these calls, pop-up messages, and emails. They want to get your money, personal information, or access to your files. This can harm your network, put your data at risk, and damage your business.

HOW THE SCAM WORKS

The scammers may pretend to be from a well-known tech company, such as Microsoft. They use lots of technical terms to convince you that the problems with your computer are real. They may ask you to open some files or run a scan on your computer — and then tell you those files or the scan results show a problem...but there isn’t one.

The scammers may then:

- Ask you to give them remote access to your computer — which lets them access all information stored on it, and on any network connected to it
- Install malware that gives them access to your computer and sensitive data, like user names and passwords
- Try to sell you software or repair services that are worthless or available elsewhere for free
- Try to enroll you in a worthless computer maintenance or warranty program
- Ask for credit card information so they can bill you for phony services or services available elsewhere for free
- Direct you to websites and ask you to enter credit card, bank account, and other personal information

LEARN MORE AT: FTC.gov/SmallBusiness
Cybersecurity for Small Business

How to Protect Your Business

If a caller says your computer has a problem, hang up. A tech support call you don’t expect is a scam—even if the number is local or looks legitimate. These scammers use fake caller ID information to look like local businesses or trusted companies.

If you get a pop-up message to call tech support, ignore it. Some pop-up messages about computer issues are legitimate, but do not call a number or click on a link that appears in a pop-up message warning you of a computer problem.

If you’re worried about a virus or other threat, call your security software company directly, using the phone number on its website, the sales receipt, or the product packaging. Or consult a trusted security professional.

Never give someone your password, and don’t give remote access to your computer to someone who contacts you unexpectedly.

What to Do If You’re Scammed

If you shared your password with a scammer, change it on every account that uses this password. Remember to use unique passwords for each account and service. Consider using a password manager.

Get rid of malware. Update or download legitimate security software. Scan your computer, and delete anything the software says is a problem. If you need help, consult a trusted security professional.

If the affected computer is connected to your network, you or a security professional should check the entire network for intrusions.

If you bought bogus services, ask your credit card company to reverse the charges, and check your statement for any charges you didn’t approve. Keep checking your credit card statements to make sure the scammer doesn’t try to re-charge you every month.

Report the attack right away to the FTC at FTC.gov/Complaint.

Learn More At:
FTC.gov/SmallBusiness
Cyber insurance is one option that can help protect your business against losses resulting from a cyber attack. If you’re thinking about cyber insurance, discuss with your insurance agent what policy would best fit your company’s needs, including whether you should go with first-party coverage, third-party coverage, or both. Here are some general tips to consider.

**WHAT SHOULD YOUR CYBER INSURANCE POLICY COVER?**

Make sure your policy includes coverage for:

- Data breaches (like incidents involving theft of personal information)
- 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
- Cyber attacks (like breaches of your network)
- 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

The FTC thanks the National Association of Insurance Commissioners (NAIC) for its role in developing this content.
WHAT IS
FIRST-PARTY COVERAGE
AND WHAT SHOULD YOU LOOK FOR?
First-party cyber coverage protects your data, including employee and customer information. This coverage typically includes your business’s 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

WHAT IS
THIRD-PARTY COVERAGE
AND WHAT SHOULD YOU LOOK FOR?
Third-party cyber coverage generally protects you from liability if a third party brings claims against you. This coverage typically includes:

- Payments to consumers affected by the breach
- Claims and settlement expenses relating 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

More insurance resources for small businesses available at www.insureuonline.org/smallbusiness
Email authentication technology makes it a lot harder for a scammer to send phishing emails that look like they’re from your company.

Using email authentication technology makes it a lot harder for scammers to send phishing emails. This technology allows a receiving server to verify an email from your company and block emails from an imposter — or send them to a quarantine folder and then notify you about them.

**WHAT TO KNOW**

Some web host providers let you set up your company’s business email using your domain name (which you may think of as your website name). Your domain name might look like this: yourbusiness.com. And your email may look like this: name@yourbusiness.com. Without email authentication, scammers can use that domain name to send emails that look like they’re from your business. If your business email uses your company’s domain name, make sure that your email provider has these three email authentication tools:

- **Sender Policy Framework (SPF)**
  - tells other servers which servers are allowed to send emails using your business’s domain name. So when you send an email from name@yourbusiness.com, the receiving server can confirm that the sending server is on an approved list. If it is, the receiving server lets the email through. If it can’t find a match, the email can be flagged as suspicious.

- **Domain Keys Identified Mail (DKIM)**
  - puts a digital signature on outgoing mail so servers can verify that an email from your domain actually was sent from your organization’s servers and hasn’t been tampered with in transit.

- **Domain-based Message Authentication, Reporting & Conformance (DMARC)**
  - is the essential third tool for email authentication. SPF and DKIM verify the address the server uses “behind the scenes.” DMARC verifies that this address matches the “from” address you see. It also lets you tell other servers what to do when they get an email that looks like it came from your domain, but the receiving server has reason to be suspicious (based on SPF or DKIM). You can have other servers reject the email, flag it as spam, or take no action. You also can set up DMARC so that you’re notified when this happens.

It takes some expertise to configure these tools so that they work as intended and don’t block legitimate email. Make sure that your email hosting provider can set them up if you don’t have the technical knowledge. If they can’t, or don’t include that in their service agreement, consider getting another provider.

**LEARN MORE AT:**
FTC.gov/SmallBusiness
Email authentication helps keep your business’s email from being used in phishing schemes because it notifies you if someone spoofs your company’s email. If you get that notification, take these actions:

**Report it**
Report the scam to local law enforcement, the FBI’s Internet Crime Complaint Center at IC3.gov, and the FTC at FTC.gov/Complaint. You also can forward phishing emails to spam@uce.gov (an address used by the FTC) and to reportphishing@apwg.org (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies).

**Notify your customers**
If you find out scammers are impersonating your business, tell your customers as soon as possible — by mail, email, or social media. If you email your customers, send an email without hyperlinks: you don’t want your notification email to look like a phishing scam. Remind customers not to share any personal information through email or text. And if your customers’ data was stolen, direct them to IdentityTheft.gov to get a recovery plan.

**Alert your staff**
Use this experience to update your security practices and train your staff about cyber threats.

**Learn More At:**
FTC.gov/SmallBusiness
Your business vendors may have access to sensitive information. Make sure those vendors are securing their own computers and networks. For example, what if your accountant, who has all your financial data, loses his laptop? Or a vendor whose network is connected to yours gets hacked? The result: your business data and your customers’ personal information may end up in the wrong hands — putting your business and your customers at risk.

**HOW TO MONITOR YOUR VENDORS**

**Put it in writing**
Include provisions for security in your vendor contracts, like a plan to evaluate and update security controls, since threats change. Make the security provisions that are critical to your company non-negotiable.

**Verify compliance**
Establish processes so you can confirm that vendors follow your rules. Don’t just take their word for it.

**Make changes as needed**
Cybersecurity threats change rapidly. Make sure your vendors keep their security up to date.
HOW TO PROTECT YOUR BUSINESS

Control access
Put controls on databases with sensitive information. Limit access to a need-to-know basis, and only for the amount of time a vendor needs to do a job.

Use multi-factor authentication
This makes vendors take additional steps beyond logging in with a password to access your network — like a temporary code on a smartphone or a key that’s inserted into a computer.

Secure your network
Require strong passwords: at least 12 characters with a mix of numbers, symbols, and both capital and lowercase letters. Never reuse passwords, don’t share them, and limit the number of unsuccessful log-in attempts to limit password-guessing attacks.

Safeguard your data
Use properly configured, strong encryption. This protects sensitive information as it’s transferred and stored.

WHAT TO DO IF A VENDOR HAS A DATA BREACH

Contact the authorities
Report the attack right away to your local police department. If they’re not familiar with investigating information compromises, contact your local FBI office.

Confirm the vendor has a fix
Make sure that the vendor fixes the vulnerabilities and ensures that your information will be safe going forward, if your business decides to continue using the vendor.

Notify customers
If your data or personal information was compromised, make sure you notify the affected parties — they could be at risk of identity theft. Find information on how to do that at Data Breach Response: A Guide for Business. Find it at FTC.gov/DataBreach.

LEARN MORE AT: FTC.gov/SmallBusiness
HIRING A WEB HOST

You may want a new or upgraded website for your business.

But if you don’t have the skills to set up the web presence you want, you may want to hire a web host provider to do it for you. Whether you’re upgrading a website or launching a new business, there are many web-hosting options. When comparing services, security should be a top concern.

WHAT TO LOOK FOR

Transport Layer Security (TLS)
The service you choose should include TLS, which will help to protect your customers’ privacy. (You may have heard of its predecessor, Secure Sockets Layer, or SSL.) TLS helps make sure that your customers get to your real website when they type your URL into the address bar. When TLS is correctly implemented on your website, your URL will begin with https://.

TLS also helps make sure the information sent to your website is encrypted. That’s especially important if you ask customers for sensitive information, like credit card numbers or passwords.

Email authentication

Some web host providers let you set up your company’s business email using your domain name (that’s part of your URL, and what you may think of as your website name). Your domain name might look like this: yourbusiness.com. And your email may look like this: name@yourbusiness.com.

If you don’t have email authentication, scammers can impersonate that domain name and send emails that look like they’re from your business.

When your business email is set up using your company’s domain name, make sure that your web host can give you these three email authentication tools:

- Sender Policy Framework (SPF)
- Domain Keys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting & Conformance (DMARC)
Software updates
Many web host providers offer pre-built websites or software packages designed to make it quick and easy to set up your company’s website. As with any software, it is essential that you use the latest versions with up-to-date security patches. Make sure you know how to keep the website’s software up to date, or whether the web host provider will do this for you.

Website management
If a web host provider is managing your website, you may have to go through that provider to make any changes — though you may be able to log in and make some changes yourself. Some web host providers may instead offer you the option of managing the website on your own. It’s important to clarify from the beginning who will manage the website after it’s built.

WHAT TO ASK
When you’re hiring a web host provider, ask these questions to make sure you’re helping protect your customer information and your business data.

☐ Is TLS included in the hosting plan? paid add-on? Will I set it up myself or will you help me set it up?

☐ Can my business email use my business website name? If so, can you help me set up SPF, DKIM, and DMARC email authentication technology? (If not, consider looking for a provider that does.)

☐ Are the most up-to-date software versions available with your service, and will you keep software updated? If it’s my responsibility to keep software updated, is it easy for me to do?

☐ After the website is set up, who will be able to make changes to it? Will I have to go through you? Will I be able to log in and make changes on my own? If I can log in to make changes, is multi-factor authentication available?
Employees and vendors may need to connect to your network remotely. Put your network’s security first. Make employees and vendors follow strong security standards before they connect to your network. Give them the tools to make security part of their work routine.

HOW TO PROTECT DEVICES

Whether employees or vendors use company-issued devices or their own when connecting remotely to your network, those devices should be secure. Follow these tips — and make sure your employees and vendors do as well:

- Always change any pre-set router passwords and the default name of your router. And keep the router’s software up to date; you may have to visit the router’s website often to do so.

- Consider enabling full-disk encryption for laptops and other mobile devices that connect remotely to your network. Check your operating system for this option, which will protect any data stored on the device if it’s lost or stolen. This is especially important if the device stores any sensitive personal information.

- Change smartphone settings to stop automatic connections to public Wi-Fi.

- Keep up-to-date antivirus software on devices that connect to your network, including mobile devices.


## HOW TO CONNECT REMOTELY TO THE NETWORK

**Require employees and vendors to use secure connections when connecting remotely to your network. They should:**

Use a router with WPA2 or WPA3 encryption when connecting from their homes. Encryption protects information sent over a network so that outsiders can’t read it. WPA2 and WPA3 are the only encryption standards that will protect information sent over a wireless network.

Only use public Wi-Fi when also using a virtual private network (VPN) to encrypt traffic between their computers and the internet. Public Wi-Fi does not provide a secure internet connection on its own. Your employees can get a personal VPN account from a VPN service provider, or you may want to hire a vendor to create an enterprise VPN for all employees to use.

## WHAT TO DO TO MAINTAIN SECURITY

**Train your staff:** Include information on secure remote access in regular trainings and new staff orientations.

Have policies covering basic cybersecurity, give copies to your employees, and explain the importance of following them.

Before letting any device — whether at an employee’s home or on a vendor’s network — connect to your network, make sure it meets your network’s security requirements.

Tell your staff about the risks of public Wi-Fi.

**Give your staff tools that will help maintain security:**

- Require employees to use unique, complex network passwords and avoid unattended, open workstations.
- Require multi-factor authentication to access areas of your network that have sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that’s inserted into a computer.
- If you offer Wi-Fi on your business premises for guests and customers, make sure it’s separate from and not connected to your business network.
- Include provisions for security in your vendor contracts, especially if the vendor will be connecting remotely to your network.

---

**LEARN MORE AT:**
[FTC.gov/SmallBusiness](https://www.ftc.gov/SmallBusiness)