AIS Network

Operationalizing Your IT Strategy

Understanding Information Security Best Practices

Understanding Information Security Best Practices

Your organization generates vast amounts of data each day — whether you know it or not.

While it is crucial to prepare for known threats to your data, applications and infrastructure, it's also vital to employ both imagination and expertise to anticipate and mitigate potential threats, many of which may not even exist yet.

The continual evolution of technology — and the threats against it — are why information security and risk management must be a part of your overall IT strategy.

Table of Contents

The Basics of Information Security

Did You Know?

47% of companies have embedded at least one instance of AI in standard processes. The more complex our systems become, the greater the threat of attack or breach.

Experts estimate that 31 billion Internet of Things (IoT) devices will be connected to the internet by the end of 2020. Our increasingly digital, automated and remote-working world means we generate more data than ever before — and rely more heavily on that data to keep our businesses running.

Information in all its forms must be protected for your business to thrive. It must be kept secure, whole and available when needed. This means taking a long hard look at your current and future risks and taking steps to minimize or eliminate their effect on you, your investors and your clients.

Threats, Vulnerabilities and Risks

Technological solutions are a key component of your information risk management program, but no technology can fully protect your systems if you don't implement them correctly as part of a comprehensive information security program.

Before you can develop a program, you need to know what you're planning for. Threats, vulnerabilities and risks may all sound like pretty much the same thing — but in the information security world, they define specific types of potential incidents you should protect against.

Threats

New incidents or events that could harm your organization. Threats can be:

- Natural (like floods or storms)
- Intentional (deliberate attacks)
- Accidental (employee error)

Vulnerabilities

Weaknesses or flaws in your systems that leave you open to threats of any kind, like:

- Unsecured networks
- Outdated employee credentials
- Unpatched firewalls or antivirus software
- Irregular or missing backups

Risks

Any potential damages you may incur when the worst happens, including:

- Financial losses
- Disruption of operations
- Reputational damage
- Legal repercussions

According to Varonis, an average of 7 million data records are compromised around the world each day.

The Ponemon Institute reports:

$3.92 million

The average data breach costs a company $3.92 million.

279 days

It takes 279 days to identify and contain a breach, on average.

25,000 records

On average, over 25,000 records are compromised in a data breach.

Information Risk Management

Information risk management is the process of preparing for and controlling the various threats and vulnerabilities that come with the use of information technology. There are two key components of any information risk management strategy:

Risk Assessment:

Identifying threats and vulnerabilities, estimating their likelihood and prioritizing risks to develop an effective response.

Risk Treatment:

Actions taken to remediate, mitigate, avoid, prevent, accept, transfer or in any way manage risks identified in the assessment phase, including establishing governance, training employees and responding to cybersecurity incidents.

Did You Know?

More than half of respondents in an Experian survey said they were enlisting the help of third-party professionals to protect their business-critical data and systems.

Developing an Information Security Program

If your company doesn't handle sensitive or proprietary data, you might think that developing an information security program isn't something you need to worry about. But you'd be very, very wrong.

While it's important to protect your clients' personal data, data breaches and cybercrime can expose you to a wide variety of losses:

- Financial Loss
- Reputation Damage
- Intellectual Property Loss
- Operations Downtime
- Customer Loss
- Stock Price Decline
- Loss of Market Share
- Employee Turnover

Did You Know?

The average cybersecurity incident takes 197 days to discover. On average, 67% of the impact of a breach is felt in the first year after it occurs, 22% in the second year, and 11% in the third year.

3 Key Factors of Information Security Program

The type of protection you need to implement will vary based on the information and infrastructure encompassed in your systems, but every information security program should cover three key factors.

Confidentiality

Sensitive information must be protected from unauthorized access and sharing. Protect your data with:

- Strong password policies
- Up-to-date encryption protocols
- Two-factor authentication
- Unique user IDs

Integrity

Data must be kept whole and uncorrupted by unauthorized changes or accidents, using:

- Carefully structured user permissions
- Access controls
- Strict version controlling
- Cloud backups

Availability

Your information must remain accessible to those who need it, even when things go wrong. This includes:

- Protecting against data loss
- Ensuring that your network is running efficiently and securely at all times

Developing a 4-Stage Strategy

Your information security program should include four main stages. Skipping any of these stages will compromise your information security program.

Prediction

Before you can protect against cybersecurity risks, you have to understand what threats and vulnerabilities you're working against. The best way to do this is by conducting an IT risk assessment and employing tools like penetration testing to identify weaknesses in your existing protections.

Prevention

Once you've identified known vulnerabilities and threats, the next step in your information security program development is to take steps to reduce the chances of an incident occurring. At this stage, it's important to establish a system of governance.

Detection

When your systems are compromised — regardless of how — the results can be catastrophic. Ensure you have regularly updated systems to monitor for unwanted intrusion so that you can respond quickly.

Response

A carefully planned and rapidly enacted incident response plan can help ensure an incident is quickly contained and the damage mitigated. The response stage of your information security program should also include recovery aspects as needed.

Assessing Your Risk

Companies of all sizes should include regular IT risk assessments in their information security programs. Don't make the mistake of thinking your business is too big to be damaged or too small to be vulnerable.

But what does an IT risk assessment look like? Start with these four steps.

1. Identify Assets

The first step in conducting an IT risk assessment is to identify your assets. Knowing what you need to protect makes it easier to determine which threats you need to be ready for. Start with a simple list of your known assets and expand it with the help of your team.

- Physical infrastructure
- Operational systems
- Data (both internal and external)
- Clients
- Inventory
- Brand reputation

Prioritize assets in order of importance to business functions. What can you least afford to lose? For example, your physical infrastructure and operational systems may be replaceable (especially if you have a disaster recovery strategy in place), but if they are out of commission how much will it set you back financially? Data is valuable (and should be backed up regularly), but would compromised data set you back temporarily or open you up to legal action?

2. Identify Threats and Vulnerabilities

Once you know what's on the line, start making a list of potential threats and vulnerabilities. Threats can encompass a wide range of events or incidents, including natural disasters, deliberate attacks or remote employees accessing systems improperly.

Vulnerabilities are any gaps in your existing security that leave you open to harm from external threats. Penetration testing can be a very useful tool in identifying previously undetected holes in your defenses.

Be sure to include people from all levels of your organization — Jane from Shipping will identify different assets and potential threats than Gina in Human Resources, and both may have great ideas for solutions.

3. Assess Impacts

Not all threats are equal. The possibility that a team member working from home might store project information somewhere insecure doesn't necessarily carry the same risk as online criminals accessing your clients' personal data and/or holding your systems for ransom.

Consider the following when assessing the potential impact of each threat or vulnerability:

- Disruption to daily operations (54% of business say this is the most significant impact)
- Financial losses (the average cyberattack costs victims over $1 million)
- Reputational damage (43% of businesses suffer brand damage after an incident)
- The threat to your clients, partners or staff

4. Prioritize Risks

Once you've identified your threats and vulnerabilities, you can begin prioritizing. Ask yourself which assets would have the greatest impact on your business if compromised and rank threats to those assets based on:

- Likelihood of occurrence
- Impact on operations
- Your ability to anticipate and prevent them

Be sure to consider any unusual circumstances. For example, if all or part of your team is working from home, the risks you face will be different than if everyone is in a shared office.

Pro Tip:

Weighing the likelihood and potential impact of a threat can feel personal. Assign numeric scores to each threat to ensure your IT risk assessment is data driven.

Cybersecurity Governance

Your systems rely on multiple delivery models, processes, vendors and data types. With greater complexity comes greater risk, which is why cybersecurity governance is so very important to your organization. Cybersecurity governance is the idea that every part of your information security risk management program should have an owner. An owner is a person or team whose responsibility it is to ensure that:

- Processes and infrastructure are regularly tested and updated for security
- Team members know how to recognize and react to incidents quickly and effectively
- Newly identified risks are correctly flagged for planners

Why Does Governance Matter?

If an aspect of your defenses has no owner, it can leave your company vulnerable to attacks from outside actors as well as current or former employees. Thoughtful governance ensures your business can:

- **Align IT operating strategies with business objectives**
- **Create effective oversight mechanisms**
- **Integrate risk and control activities**
- **Optimize resources**
- **Streamline business and auditing processes**
- **Collect higher quality assessment data for future security refinements**

4 Steps to Reduce Your Risk

An effective cybersecurity governance strategy isn't difficult to implement. In fact, it's much less complex than the systems that necessitated governance in the first place. But it must be developed in a thoughtful way.

1. Define policies and goals

Clearly define your risk management policies, strategies and goals upfront. This will provide a comprehensive roadmap for your cybersecurity governance plan. Ensure policies and goals are widely communicated and understood across your organization.

Key components of this step include:

Understanding Risks	Defining Goals	Establish KPIs
A risk assessment will help you identify and prioritize threats and vulnerabilities	Clarify what level of risk is acceptable and what you'll do to achieve a comfortable level	Define how you'll measure success — you can't improve what you don't measure

2. Standardize processes

By standardizing procedures across your organization, you reduce your overall risk. Make sure there's a clear, widely communicated process for adding or changing:

- Operating systems
- Devices
- Applications
- Software
- Network configurations

Standardization makes it easier for you to maintain security by eliminating the need to monitor, troubleshoot and protect a patchwork of different devices and solutions.

3. Lead from the top

The only way your cybersecurity governance program will succeed is with buy-in from top-level leadership. Ensure that your governance plan:

- Fits other organizational goals
- Includes a commitment from leaders
- Is fully documented and available for all team members

4. Empower enforcement

Once you've made and trained your plans, designate someone to oversee your cybersecurity governance program and give them the power to enforce it. A CISO may be a good choice.

Creating a Cybersecurity Training Program

Cybercrime is on the rise and you're only as strong as your weakest link — which is why cybersecurity awareness training is a must-have for your organization.

Phishing scams have increased dramatically as criminals seek to prey on employees working remotely because of the COVID-19 pandemic. And KnowBe4's 2020 Phishing By Industry Benchmarking Report suggests that 38% of employees who don't undergo cybersecurity awareness training will fall victim to phishing scams.

Your team members must:

- **Be aware of potential threats**
- **Be able to recognize threats**
- **Know how to prevent incidents**
- **Know what to do when prevention is impossible**

Did You Know?

Not sure if cybersecurity training for employees is worth the investment? Think of it as a human firewall — close to 90% of data breaches are caused by human error.

Creating a program of regular cybersecurity awareness training should be a key part of your information security program. Without that and an effective cybersecurity governance plan, you run the risk of falling victim to threats and vulnerabilities caused by a lack of adequate prevention or incident response.

The Basics of Cybersecurity Awareness

Your training program should cover these five fundamental facets of cybersecurity to limit the likelihood of your employees contributing to a breach:

Physical Security

Your sensitive information and infrastructure must be protected from unauthorized physical access. It's important for your staff to understand physical security policies, whether they are working in the office or remotely. Policies can include:

- ID badges/swipe cards/biometrics
- Guest logging
- Alarms and surveillance
- Device lockup

Measures to secure your systems physically can appear inconvenient when they're first introduced, so it's crucial that your team understands the value of the policies. Team members who believe in a system are far more likely to maintain it than those who only see it as a nuisance.

Password Security

It's important to educate your staff on the risks related to easily cracked passwords, and teach them best practices for credentials management.

- Create strong passwords that include both uppercase and lowercase letters, numbers, and symbols
- Avoid obvious passwords like birthdays, children's names, or things like "password" or "12345"
- Two-factor authentication using email or text can help protect systems when passwords are compromised
- Don't reuse passwords, and use a different password for each account you access

Make sure your team knows that every new device or bit of infrastructure needs new secure credentials, no matter how non-critical a component of your network it may seem.

Threat Recognition

Your team can't respond to threats that they can't identify. Be sure your cybersecurity training includes examples of all the risk types that could affect your business:

- **Phishing:** A new phishing site goes live every 20 seconds
- **Social Engineering:** 33% of hacks in 2018 relied on social engineering
- **Malware and Viruses:** 60% of breaches involve a vulnerability that could have been patched
- **Physical Intrusions:** 42% of security professionals have concerns about their company's ability to secure physical spaces containing critical data

---

Reporting

Regardless of the type of communications system you use for reporting cybersecurity incidents, make sure your team understands how and when to use it, and who to notify if an incident occurs.

Open communication is key here — your team must feel safe and empowered to tell someone if they detect an issue (past, present or future), even if it's just a suspicious email.

Incident Response

The incident response plan component of your cybersecurity training program should include practical scenarios in addition to instruction on documented policies. Staff should understand exactly what their responsibilities are regarding:

- Prevention
- Detection
- Containment
- Remediation

Make sure you include some real-life examples of possible incidents. You'll get insight into how your staff responds in a crisis and identify areas that need improvement.

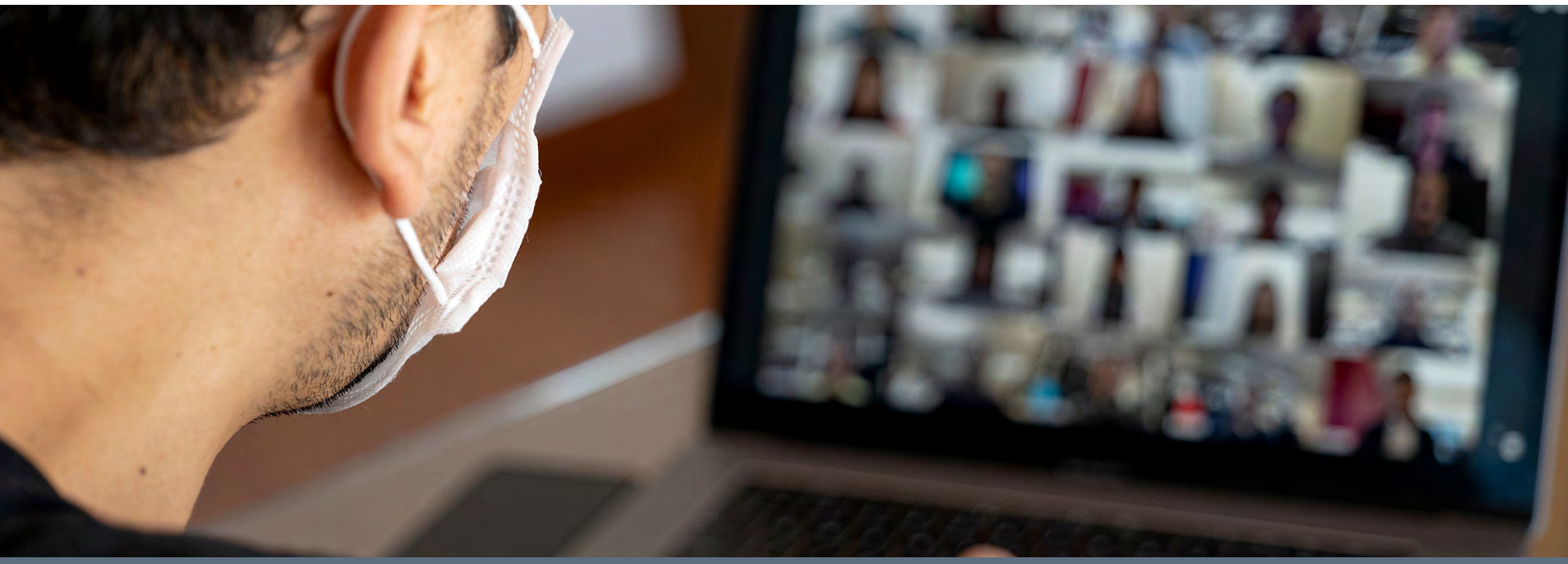
Finding the Right Instructors

Depending on your company's specific cybersecurity needs and goals, you may want to pursue certification for your organization (or for individuals). Or, if certification doesn't seem like something you need right now, you may prefer to work in-house on something simpler.

Cybersecurity instructors can be from your own team, external experts or a combination of both. There are some areas of cybersecurity awareness training that are best taught by a certified external instructor, while others can be handled internally.

Responding to an Incident

We see headlines about network penetrations nearly every day, highlighting the ever-evolving nature of data security. Malicious and criminal intrusions can happen to businesses of all sizes, and a global crisis only exacerbates the risk. Experts say cybercrime has increased by as much as 30,000% during the COVID-19 pandemic.



Did You Know?

- EasyJet is facing a multi-billion dollar lawsuit over a breach that compromised the data of at least 9 million customers
- 8 million Home Chef customers had their private data accessed in a recent breach
- More than 15 billion records were exposed by data breaches in 2019

There are two fundamental areas you should consider when planning information security incident responses: proactive and reactive. Proactive prevents incidents. Reactive is where disaster recovery comes in — something has happened, so what are you going to do?

Identify and test policies, processes and infrastructure for threats and vulnerabilities to understand what areas need improvement. But being prepared for an incident can also include training staff about their roles and responsibilities in protecting your company and regularly reviewing your plan and the protections you have in place to make sure they're up to date.

5 Steps for Incident Response

Let's face it — controls can fail. Having the right incident response steps in place can minimize the damage. Here are 5 to consider.

Identification

Requires monitoring so irregularities are flagged quickly. You'll need to determine:

- Type of attack
- Severity
- Other Impacts (Has the incident put you in violation of standards or contracts?

Containment

Time is of the essence. Your response should include:

- Shutting down programs and systems
- Identifying and removing malicious code and/or persons
- Updating protections as needed

Remediation

- Ensure all artifacts of the incident have been removed
- Repair or update systems
- Check all patches are current
- Ensure backups are functioning properly

Recovery

Continuous monitoring is critical to ensure that the incident has been fully resolved and no further threats exist. Restore systems from backup and resume operations, documenting all steps you take.

Assessment

Compile a report of the incident using the record of your response. This will help ensure similar events do not happen again in the future, and help in the event of litigation.

Some questions that can help in your assessment (and future preparations) include:

- Are systems currently secure? If not, what isn't and what needs to be done to secure it? Triage based on importance.
- What effects has the incident had, and are further effects expected?
- How was the system breached?
- What response steps have been taken, and have they had any peripheral impacts?
- What response steps remain to be implemented?
- Which stakeholders and governors should be involved in planning new strategies?

Minimizing Your Downtime

A comprehensive availability and disaster recovery plan includes strategies to provide a stable network and protect data from interception and loss during disasters — whether man-made or natural. Data lost to hackers or hurricanes can cost you dearly while damaging your reputation and exposing you to unnecessary financial and legal risks.

Did You Know?

- 94% of companies do not fully recover from severe data loss
- The cost of downtime can range from $10,000/hour to over $5 million/hour

Ensure Availability

Availability management is at the core of any IT service management plan and closely correlates with service value. Unrecoverable data loss can have severe repercussions for your organization, including lost revenue, a damaged reputation and even litigation.

What can affect the availability of your data and systems?

- Hardware failure
- Human error (average cost: $3.5 million)
- System failure
- Natural disaster
- Computer virus (90% of malware has evolved to circumvent defenses)
- Theft
- Accidental deletion
- Power outage (Downtime costs between $10k and $5M per hour on average)

Waiting for an incident to occur — or for regulatory bodies to force your hand on compliance — can be a costly mistake. Any plan is better than no plan at all, and developing an availability and disaster recovery plan doesn't have to be complex. An information security officer can help you formulate one.

Create a Disaster Recovery Plan

The development of a business disaster recovery plan should be an integral part of your information security program. A strategy for how to deal with a cybersecurity incident is incomplete if it doesn't include steps for maintaining system and data availability.

Did Your Know?

The COVID-19 pandemic has created considerable new risk for businesses who were unprepared for widespread off-site work — those with existing availability and disaster recovery plans had lower risk of security incidents, or were better-prepared when incidents occurred.

Development of a robust IT disaster recovery plan will include the following three steps:

1

Business Impact Analysis

- Review existing business continuity capabilities
- Identify critical business functions and their dependencies
- Estimate the impact of disruptions
- Estimate the timeframe for recovery

2

Strategy Development

Understanding dependencies is vital here. If System A is critical to your operations, obviously it must be protected. But if System A is dependent on System B, then System B must be equally protected.

Ensure your strategy includes necessary IT resources, security concerns and data retention solutions.

3

Documentation

The final step in creating your IT disaster recovery plan is documenting it fully, and adding it to your cybersecurity awareness training program. Include:

- Points of contact
- Instructions for recovery team and management
- Plans for reviews, updates and future training

Securing Your Network

One of the truths of business is that the speed of change is inverse to the size of the organization — so the organizations that maintain large compliance frameworks will tend to lag behind the individuals or small groups who leverage their agility to create new threats.

Did You Know?

Some extremely tech-savvy companies have experienced some of the biggest data breaches in recent history.

Be secure, and compliance will fall into place. Just be compliant, and you're only secure against yesterday's threats. Securing your network and data means securing your network firewalls and routers.

Physical Devices

Workstations, laptops, smartphones, servers, the cables your data moves through, are all potential vectors for a network intrusion. Physical devices must be protected to maintain strong router and network firewall security. There are a few things you can do to ensure your network is as safe as possible:

Limit Permissions

Restrict permissions for key parts of your network to those who:

- Need access to perform their job
- Have appropriate skills
- Are reliable

Establish Controls

Create a control program that documents access and actions so you can:

- Assess ongoing incidents
- Anticipate future problems
- Investigate incident causes and responses

Assign Responsibility

Make sure your leaders have the skills and access to:

- Assess vulnerabilities
- Maintain software
- Review and update configurations

Review Configurations

Regularly review device configurations and update software for wireless access points, firewalls, switches and routers.

Create Use Policies

Work with your team and experts to establish policies that define acceptable uses of technologies.

Monitor Access Points

Keep tabs on who is accessing your system remotely, and from where.

Pro Tip:

A change to your network could mean a physical change like adding a new device, or a software-related change like a firmware or anti-virus update.

Software Protections

Keep Your OS Current

Your operating systems should be continually updated to leverage the power of new technologies, fix bugs and address security vulnerabilities discovered over the course of their lifecycle.

Apply the Principle of Least Privilege

The principle of least privilege suggests that anyone who requires access to a system be given only the lowest level of permissions possible to perform their task — and for the shortest possible duration.

Enact Hardening Standards

Maintain a detailed set of hardening standards. Numerous standards — like SANS, NSA or NIST — already exist to help you protect yourself.

Log Configuration Changes

It's essential to keep a record of who makes changes to your systems — this frequently-missed step can be useful when determining whether an event is the result of a security incident, human error or authorized action.

Change Default Settings

Your systems have a lot of settings that affect them in ways you wouldn't expect. Leaving network settings in their default state gives intruders a door they may already have the key to.

Schedule Regular Updates

Be sure to include networking devices' software in your updating schedule and make regular patching a key part of your defense against intrusion.

Encrypt. Encrypt. Encrypt.

Encryption makes it far more difficult for cybercriminals to use any data they successfully intercept, but a lot of encryption protocols have already been broken to the point of obsolescence. Stay current using these best practices:

- Disable web-based management (if you aren't using it)
- Verify that your certificates are strong and accepted
- Disable Telnet and clear text protocols
- Use the latest SSH whenever possible
- Establish a VPN

Pro Tip:

Check with your network administrator to determine whether your current encryption protocols meet your needs and schedule regular security reviews. It's better to be too secure than to lose important assets or time.

Other steps you can take to protect from intrusions include:

Remote Console Timeouts

Timeouts of 15 minutes or less can protect you from malicious acts when users are away from devices. An easy keyboard lock shortcut is a huge help.

Support NTP

Network Time Protocol synchronizes computers to UTC and utilizes algorithms to properly coordinate time between hosting time servers so you know when your system is accessed.

Disable Unused Interfaces

Disabling unused interfaces can help prevent intruders from using old forms or APIs to access your network.

Verify Downloads

It's essential to keep a record of who makes changes to your systems — this frequently missed step can be useful when determining whether an event is the result of a security incident, human error or authorized action.

Restrict Inbound/ Outbound ICMP

Limit unauthorized network infrastructure exposure while still reaping the benefits of network monitoring.

Enable Anti-Spoofing Rules

Prevent bad actors from fooling your system into believing they're within your trusted network.

Traffic Rules

Traffic rules dictate what's allowed to pass in and out of your network. They're an instrumental part of your router and network firewall security strategy. Let's take a look at some steps you can take to reduce the risk of data and other assets being lost or accessed via your network.

Use Approved Ports and Services

Ensure no one can find unprotected points of access directly or via unreliable software. Work with your network administrators to maintain a list of approved ports and services.

Limit Traffic

Limit types of data that enter and exit your network by specific means. Work with your network administrator to create policies for information traveling in or out.

Avoid "Any"-Based Rules

Rules based on "any" (an easily circumvented coding catch-all) can't shape traffic securely. Assess specific risks most relevant to your organization and ensure they're covered effectively.

Securing Systems for Remote Work

A flexible information risk management program is critical, as the risks your organization faces continually evolve, and the COVID-19 pandemic has revealed a security vector often overlooked by many businesses: the security risks of remote work.

Staff are working from home in record numbers in an attempt to weather the pandemic and comply with lockdown orders and social distancing guidelines. But the virus isn't the only threat they're facing. Whether you have a return-to-office plan or not, odds are that people will be working from home more going forward than they have in the past.

With so many employees working from home, business networks are being tested in entirely new (and often unexpected) ways. Traffic loads are different, people are accessing shared files in new ways, and communicating using untested tools. It's important to be prepared, unless you're willing to lose important staff on the basis of workplace safety.

Did You Know?

86% of executive team members say data breaches are more likely when employees are working out of the office. 57% of CIOs suspect their mobile workers have been hacked in the last year.

Cybersecurity Risks

What kind of information security risks are associated with remote work? The specific threats and vulnerabilities your organization faces will vary based on the nature of your business, your systems and what kinds of data you collect.

Unsecured Network Access

In your offices, you can maintain full control over your company's networking and Wi-Fi to prevent unauthorized parties from accessing your business-critical systems or data.

Working from home means your employees are using their personal Wi-Fi networks, which are unlikely to include such stringent security measures.

Unsecured Devices and Programs

While company-owned devices can be regularly inspected and updated to ensure your security standards are maintained, one of the cybersecurity risks of remote work appears when your team uses devices, programs or platforms not officially sanctioned by your IT department.

"Shadow IT" — when your employees solve new problems on their own by adopting untested solutions — can dramatically increase the risk of your data or systems being compromised.

Phishing Scams

Scams in which online criminals pose as people or organizations your employees might trust with sensitive data have skyrocketed since the pandemic began.

When regular in-person meetings or conversations can't happen, your staff may not question an email request that appears to come from within the company.

Security Maturity Assessment

Mature security not only includes countermeasures you need today, but also ensures the flexibility to counteract new situations as they arise. Companies that are ready for abrupt changes in their regular IT risk assessments — even if they don't know what those changes might be — have a significant edge over those who only have a locked-down plan to deal with their known attack vectors.

The information security threats your organization faces are continually evolving. And experts predict that working from home won't automatically disappear from most industries when the pandemic ends. That's why the cybersecurity risks of remote work are something you should prepare for in the long term.

Did You Know?

Attackers are constantly updating their skills and toolsets. The 2020 State of Malware Report shows the following threats increased in 2019:

Adware
+463%

RiskwareTool
+52%

Backdoor
+14%

Hacktool
+224%

A security maturity assessment isn't just a list of items you can check off once and be done with them. It's an ongoing system of internal checks, attack vector and response research, regulatory maintenance and standards updates.

Done right, it can provide your management team with valuable insight into your strengths and weaknesses and illustrate the value of current and future investments in information security.

Make sure your assessment of security maturity includes:

- Connected devices and networks
- Threat intelligence
- Governance
- Compliance and standards requirements
- Disaster recovery
- Incident response strategies

Penetration Testing

Employing new digital technology to streamline and automate your processes, and facilitate remote working, is a great way to keep your costs down and service levels up, especially now — but new technologies bring new vulnerabilities. Regular penetration testing can help ensure your systems are correctly strengthened against threats, and that your data is secure.

Penetration testing is the best way to uncover your vulnerabilities and determine whether or not they can be exploited. Regular penetration testing can help ensure compliance with government and industry regulations and certification frameworks.

Did You Know?

16% of security vulnerabilities in tested applications are a medium, high or critical risk.

Penetration Testing vs. Vulnerability Scanning

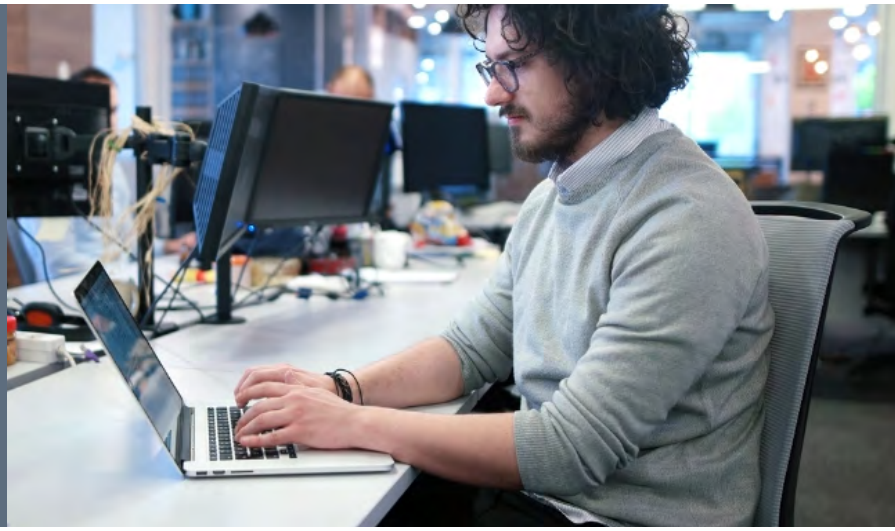
The key difference between penetration testing and vulnerability scanning is the determination of exploitability. Identifying vulnerabilities is important, but knowing if they can actually be used against you can help determine how much money and time you should dedicate to remediating the issue.

Pen testing can expose a variety of security issues, including:

- **Encryption Problems:** An unsecured database left 425GB of data exposed in 2019
- **Backdoors**
- **Weak Passwords:** 65% of users use the same password for multiple accounts
- **Outdated Software:** Including unpatched operating systems
- **User Behaviors:** Insider threats have increased by 47% since 2018
- **Application Flaws**
- **Improper Network Configurations:** A poorly configured network exposed 8TB of user data on a French news outlet

Pro Tip:

It's crucial to test security from both inside and outside your network. Different vulnerabilities will exist outside your firewalls than exist inside, so be sure to include both in your penetration testing plans.



Implementing a Pen Testing Strategy

It's important to schedule regular pen tests — penetration testing is not a "one and done" solution. A system that is secure today doesn't guarantee impermeability against new threats next week, next month or next year.

Did You Know?

Studies have shown that 86% of vulnerabilities can be patched within 24 hours, so regular testing can definitely improve your information security.

Your penetration strategy can be broken down into five main stages.

1	**Planning**	Identifying tools to be used and gathering intelligence on systems to be tested
2	**Scanning**	Examining system code in both static and dynamic states
3	**Simulated Attacks**	Staging system attacks to see where vulnerabilities exist and can be exploited
4	**Maintaining Access**	Seeing if vulnerabilities permit persistent access — long enough for damage to occur
5	**Analysis**	Detailing vulnerabilities discovered, data accessed and duration of the breach

Types of Penetration Testing

Just as there are different ways for bad actors to exploit vulnerabilities in your systems, there are different types of penetration tests you should conduct.

Internal

Internal vulnerabilities can come from disloyal staff or compromised credentials

External

External vulnerabilities can appear in websites, applications, email and DNS

White Box

Hacker has some information about security measures beforehand

Black Box

Hacker has no information about security measures beforehand

Covert

Organization officials are unaware that testing is being conducted

Benefits of a Chief Information Security Officer

The consequences of failure in keeping ahead of the cybersecurity curve can be severe. Having someone on your team who specializes in information security — even on a part-time or virtual basis — can be helpful in many aspects of your cybersecurity strategy.

Did You Know?

86% of companies properly staffed with cybersecurity expertise employ a Chief Information Security Officer.

With specialized training and a steady eye on the evolving threat landscape, a part-time virtual Chief Information Security Officer (vCISO) can help your organization move forward safely as you embrace technological developments. They can also help protect you from loss and cement your reputation as a business with the right mindset toward cybersecurity.

What Does a CISO Do?

Assessment

- Assessing the state of the cybersecurity strategy and identifying strengths and weaknesses in its design and implementation

Development

- Developing and driving the implementation of key initiatives to close gaps, build on existing strengths and correct weaknesses
- Leading development, approval, implementation, and periodic updates of information security policies, procedures, standards and guidelines
- Partnering with enterprise architecture, infrastructure and application development teams to ensure that technology solutions align with cybersecurity policies and standards

Oversight

- Ensuring your cybersecurity program is compliant with legal, regulatory and contractual requirements
- Establishing and overseeing vulnerability management, including regular vulnerability scanning, penetration testing, and the coordination of remediation activities
- Overseeing incident response planning and breach investigation activities

Instruction

- Providing expertise on security standards and best practices
- Monitoring external threat intelligence sources and advising stakeholders on appropriate courses of action
- Training staff and board members to elevate their understanding of privacy, cybersecurity risk issues and processes

Why a Virtual CISO?

Just as the popularity of shared offices and infrastructure was rising before so many of us started working from home, the "only pay for what you need" model has become a go-to for many successful businesses. You get the expertise and oversight of a CISO, but you only pay a fraction of their salary. It's a win-win.

You have a couple of options if you're looking for a vCISO: you can hire a freelancer or contract the services of a partner that provides CISOs as needed. There are pros and cons to working with freelancers.

Freelancer Pros

- Expert knowledge
- Previous experience
- Affordable

Freelancer Cons

- Availability is not guaranteed
- Onboarding times can vary if they're used to systems that differ from yours

While freelance CISOs and vCISOs can offer some benefits to organizations that aren't prepared to shoulder the cost of adding a full-time team member, working with a vCISO from your managed services provider offers those same benefits and more.

Availability

A vCISO will provide the cybersecurity expertise and oversight you need when you need it — not when they have time.

If you're facing a critical incident and unsure of next steps, do you want to wait around for answers? If your organization has experienced a breach, you need someone with 24-7 availability.

Reliability

Cybersecurity experts are some of the most highly sought-after members of the technology world. They're also some of the most stressed. A vCISO from your MSP is less likely to burn out because their load can be shared by colleagues.

Governance

Without a dedicated CISO, the task of overseeing your ever-evolving security measures and addressing threats and vulnerabilities may fall to a team member who lacks the authority to implement changes and ensure compliance.

Cyber Forensics and Litigation

Cybersecurity attorneys play a critical role in protecting their clients from the damages associated with data breaches, but it's hard to keep abreast of changes in both technology and law. A cyber forensics consultant can help.

Cyber forensics experts can collect and preserve evidence from networks, applications and devices that can be used to defend clients against litigation if their IT systems are compromised.

Did You Know?

When you partner with a properly certified cyber forensics consultant, the information they uncover belongs to you — meaning it is protected by attorney-client privilege.

Communications and data-handling technology is developing faster today than ever before. And companies around the world have faced hefty lawsuits for failing to adequately protect their customers' data.

A cyber forensics consultant can help legal professional protect their clients by:

Identifying Potential Issues

- Identify strengths and weaknesses in architecture. documentation, and implementation
- Ensure an information security program is compliant with all legal, regulatory, and contractual requirements
- Provide cybersecurity assessment and auditing services

Providing a Legal Perspective on Operations

- Drive implementation of key initiatives to address weaknesses and build on existing strengths
- Lead development of policies, procedures, standards and with an eye toward litigation
- Establish or improve vulnerability management programs

Guiding Information Security Leaders

- Ensure adequate governance of cybersecurity measures
- Oversee incident response planning and breach investigation activities with an eye towards potential legal ramifications

The Right Information Security Partner for You

At AISN, our strategies are based on The National Institute of Standards and Technology's Cybersecurity Framework, a voluntary system of standards, guidelines and practices that promote the protection of critical infrastructure.

AISN is a Virginia SWaM-certified leader in cloud enablement, information security and risk management, managed services, and award-winning application development with a wide footprint in Virginia government as well as large corporations across North America.

We offer expert support in developing and implementing a risk management program from risk assessment to penetration testing to employee training. If you've got cybersecurity questions, get in touch with us today.

CONTACT US

AIS Network
919 E. Main Street, Suite 1000, Richmond, VA 23219
www.aisn.net | sales@aisn.net | 888-401-AISN