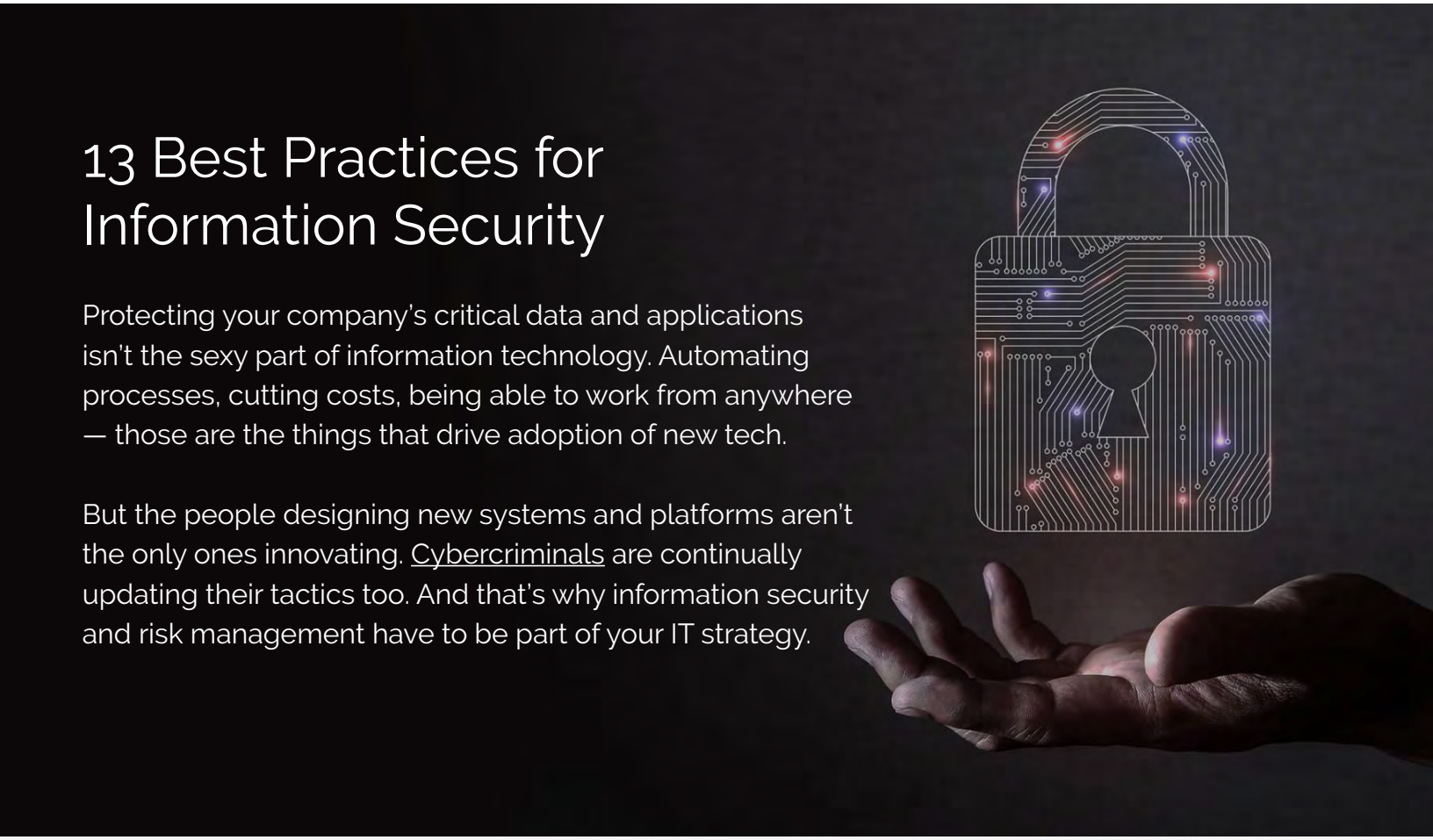
13 Best Practices for Information Security



Protecting your company's critical data and applications isn't the sexy part of information technology. Automating processes, cutting costs, being able to work from anywhere — those are the things that drive adoption of new tech.

But the people designing new systems and platforms aren't the only ones innovating. Cybercriminals are continually updating their tactics too. And that's why information security and risk management have to be part of your IT strategy.

Table of Contents

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

1. What Is Information Risk Management?

First things first. Information risk is the probability that your systems will be compromised and someone or something will negatively affect your data's confidentiality, integrity, or availability. Information risk management includes the strategies you employ and the methods you use to mitigate the likelihood of your data or systems being compromised.

Three Areas Your Information Security Strategies Should Cover

Threats

Incidents or events that could compromise the security of your network, including natural threats, intentional threats and unintentional threats

Vulnerabilities

Weaknesses in your systems — whether physical or digital — that leave your company open to damage

Risk

The potential for damage you face when threats find vulnerabilities, including financial loss, operations disruption, reputational damage and more

To protect yourself, your partners, your clients and your business from the risks you face, your information security program should include careful assessment of risks, a clear strategy to mitigate them and a plan for quickly containing the damage when breaches occur.

Want to know more? Check out our post "What Is Information Risk Management Really About?"

Read Articles

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

AIS Network

Did You Know?

According to the FBI's Internet Crime Report, over $3.5 billion was lost to cybercrime in 2019.

$3.5 billion lost to cybercrime

2. Performing an IT Risk Assessment

Do you really need an IT risk assessment? Surely if you're compliant with industry and government regulations and standards your data must be secure. Unfortunately, compliance does not equal security. Cybersecurity threats are evolving as quickly as the technology itself and regulatory bodies are simply not agile enough to keep up with new threats.

So how do you determine what risks your organization is facing? Performing an IT risk assessment can help you get a clear picture of threats, vulnerabilities and risks in four easy steps.

Step 1
Catalog Assets

Work with your team to develop a list of all the assets you need to protect.

Step 2
Identify Threats and Vulnerabilities

Examine your security systems for gaps and weaknesses.

Step 3
Assess Impacts

This can include disruptions, financial costs, reputational damage, legal issues and more.

Step 4
Prioritize Risks

Rank risks based on how likely they are to happen, the impact they will have, and whether or not you can prevent them.

Make sure your assessment includes all possible situations. Just because no one on your team is working remotely right now, doesn't mean it will never happen.

Take a look at "How to Perform an IT Risk Assessment" for more information on laying a solid foundation for your information security strategy.

Read Articles

Did You Know?

Businesses that make information security a part of regular operations are 4.3 times better at preventing cybersecurity incidents.

3. Remote Work Cybersecurity Risks

The advantages — and risks — of having employees work remotely have been thrust into the spotlight in recent months as the COVID-19 pandemic forced many businesses to close their doors. Experts suggest the trend of remote working will likely continue long after the virus is gone. Whether your organization has a strategy for reopening or not, protecting your systems against some of the information security risks that come with remote work is a critical part of a mature cybersecurity strategy.

Information security risks specifically associated with remote working include:

Unsecured Networks

Most home wifi networks have weaker security protocols than those in office environments

Unsecured Devices or Programs

90% of working adults use devices issued by their workplaces for non-work activities

Phishing Scams

94% of malware is delivered via emails opened by unsuspecting recipients

How can you tell if your information security program is up to the challenge of handling ever-evolving threats posed by negligent staff or malicious online criminals? A mature information security strategy is one that includes flexibility to adapt to new situations or threats.

"Are You Prepared for the Cybersecurity Risks of Remote Work?" Check out our blog post for more information on developing a mature information security program.

Read Articles

Did You Know?

You can measure the maturity of your information security program by seeing how well you handle the 4 Ps: **Protection**, **Prevention**, **Preparation**, and **Preemption**.

4. Developing Your Information Security Program

Understanding the need for a cybersecurity strategy is one thing. Developing a comprehensive information security program is quite another. Where do you even start? If the prospect seems unduly daunting, consider the cost of not having one. Some 445 million online cyber fraud and abuse claims were reported in the first quarter of 2020, and the average data breach costs $3.92 million.

Develop your information security program in four basic stages.

Prediction

Use risk assessments and pen testing to identify threats and vulnerabilities.

Prevention

Close security gaps and implement policies to minimize risk.

Detection

Deploy monitoring systems to identify data breaches as soon as they occur.

Response

Create a clear action plan so that breaches are quickly contained and remediated.

Remember, the loss or theft of privileged or business-critical information isn't the only factor your cybersecurity plans should cover. Make sure your strategy can protect the confidentiality, integrity and availability of your data and systems.

In "How to Develop an Information Security Program," we'll go into more detail on how you can make sure your information security program is ready for anything.

Read Articles

Did You Know?

Juniper Research predicts that the total number of IoT connections will reach 83 billion by 2024. Having a comprehensive strategy will make it easier to adapt to new developments and technology.

83 billion IoT connections

5. The Importance of Cybersecurity Governance

As the complexity of your systems increases with the adoption of new technological solutions, so must the measures you take to keep those systems secure against intruders. But the most carefully designed information security program will fail without adequate leadership. Some two-thirds of organizations ignore more than 25% of security events.

If no one person or team is tasked with taking responsibility for your program — or any one part of your program — it's easy for aspects to go overlooked. Establish governance by assigning responsibility directly to someone empowered to enforce policies and make changes in each of these areas.

- **Regularly testing and updating security measures**
- **Training employees to identify and react to information security incidents**
- **Identifying and flagging new risks for follow-up**

A system of cybersecurity governance can help protect your organization from threats while also optimizing resources, streamlining processes and ensuring the security strategies align with your company's business goals.

For more on the value of governance and how to implement a governance program, check out "Why Cybersecurity Governance Matters to Your Organization."

Read Articles

Did You Know?

A survey conducted by Forrester Consulting found 77.4% of respondents report a poor relationship between IT and security departments.

6. Implementing Information Security Training

With a comprehensive information security plan and the governance to lead and oversee it, you can begin working on ensuring all members of your team — from the lowest-ranking administrative assistant to your C-suite — understand the risks your company faces and the policies you've implemented to mitigate those risks.

A good cybersecurity awareness training program can help improve compliance with information security policies that, if not clearly explained, may appear inconvenient and unnecessary to your team. Make sure your employees understand policies that govern:

Physical Access

Can include ID badges, guest logging, alarms and device security

Passwords

Two-factor authentication, password requirements

Identifying Threats

How to recognize online scams, phishing, malware and more

Reporting

When to escalate cybersecurity concerns and who to report them to

Information threats are continually evolving, so don't treat training as a one-and-done task. Training should be offered on a regular schedule to refresh memories and keep your team abreast of new policies and threats.

Not sure where to start? Read our post on "How to Implement a Cybersecurity Awareness Training Program" for more information.

Read Articles

Did You Know?

80% of organizations have experienced at least one successful cyberattack. Most cite worrisome employee behavior as their greatest challenge.

7. Maintaining Availability

Keeping your data and systems online at all times is critical to the success of your business. The cost of downtime continues to climb. And as remote working gains popularity, keeping your networks live and your systems accessible to employees will become increasingly important.

Availability can be compromised by a range of factors:

Hardware or System Failure

Employee Error

Theft

Natural Disaster/ Power Outage

Malware

Fortunately, you can dramatically decrease your risk of downtime — and associated disruptions and losses — by developing an availability strategy and employing a disaster recovery strategy. Identify your current continuity capabilities and the impact of any potential disruption, and then develop a clearly outlined plan of action. You can't necessarily prevent a downtime incident, but you can make sure you're not one of the 43% of businesses that never reopen afterward.

Read "How to Protect Your Assets With a Disaster Recovery Plan" to learn more about availability and DR strategy.

Read Articles

Did You Know?

The Ponemon Institute reports that only 24% of cybersecurity pros actually focus on preventing incidents, rather than reacting to them.

8. Responding to an Information Security Incident

The odds are fairly high that at some point your organization will fall victim to an information security incident. There are more than one billion identified malware programs in existence and a cyberattack occurs once every 39 seconds. (And that's assuming that your incident is the direct result of an attack, rather than a hardware failure or employee negligence!) Think of your systems being compromised as a "when" not an "if."

But the right preparations can help minimize the impact of any sort of breach and quickly get your company back to business as usual. Your cybersecurity incident response plan should include these five basic steps.

Detection

Identify and document the details of the incident.

Containment

Contain the breach, quarantine affected systems and remove anyone involved.

Remediation

Remove any malware, repair damage and test systems and backups.

Recovery

Restore systems from backups and resume operations cautiously.

Assessment

Determine how, when and why the incident occurred and how to prevent it from recurring

In "5 Cybersecurity Incident Response Steps You Need to Know," you'll find detailed information on how to minimize the impact of an information security incident.

Read Articles

Did You Know?

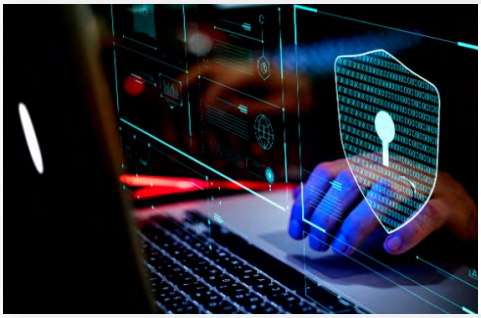
The average data breach costs $3.92 million — $150 per record compromised.

9. Router and Network Firewall Security

Router and network firewall security is the first line of technological defense protecting your business from outside intruders. But regular maintenance, testing and updates are critical if you want to keep your organization safe.

Devices	Operating Systems	Traffic
Work with your team to develop a list of all the assets you need to protect.	Regularly patch, update and test operating systems, control access privileges and log any changes to keep operating systems secure.	Limit and monitor traffic that can enter and exit your network and regularly inspect for unguarded access points.

Don't make the mistake of thinking your organization is too big or too small to be a target. More than 15 billion records were exposed by data breaches in 2019, and the targets were companies of all sizes.



Check out "Network Firewall Security: Are You Compliant or Are You Secure?" for more information on reinforcing network firewall security.

Read Articles

Did You Know?

Each of the 15 largest recorded data breaches compromised the records of more than 100 million people.

10. Penetration Testing

A key aspect of your information security program is regularly inspecting your systems for vulnerabilities that could be exploited by new threats. Penetration testing is a valuable weapon in your arsenal against cybercrime. While vulnerability scanning only locates gaps in your security, pen testing lets you see just how far into your system a hacker could get by exploiting those gaps — giving you a clear, measurable indication of risk.

There are five different types of pen testing and each provides different insights.

Internal

Testing vulnerabilities from within your organization

External

Testing vulnerabilities that outside actors could access

White Box

The tester has some knowledge of the security you have in place

Black Box

The tester has no knowledge of the security you have in place

Covert

Your team is unaware of the test (and therefore can't prepare for it)

Penetration testing under a variety of scenarios can help you identify holes in your security and provide a complete picture of the potential damage that would result if they were exploited. This is especially useful when prioritizing which vulnerabilities to address first.

For more information on how pen testing works, take a look at "You Need the Security Benefits Penetration Testing Can Offer."

Read Articles

Did You Know?

Experian's Seventh Annual Data Breach Preparedness Study found that 57% of companies regularly conduct security assessments with the assistance of outside experts.

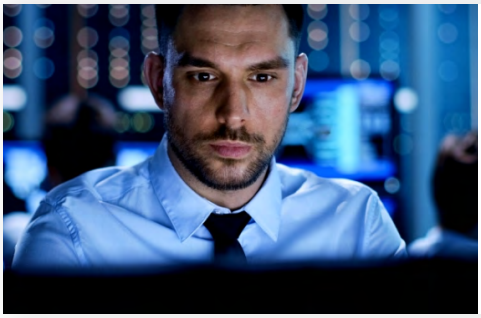
11. What Is a vCISO?

The information security risks your business faces are continually increasing as your organization grows and adopts new technology solutions. And experts estimate that more than 60% of businesses are operating with understaffed cybersecurity teams. The best way to ensure that you're prepared for existing and evolving threats to your expanding systems is to employ a Chief Information Security Officer, or CISO.

But what if you simply don't have the budget for a full-time cybersecurity executive? A vCISO — an expert who can head up your information security program while operating much like a consultant — might be the answer. What does a vCISO offer?

- **Expertise:** Experienced and trained in the latest threats, vulnerabilities and best practices
- **Affordability:** Less expensive than hiring a full-time officer, but value isn't compromised
- **Reliability:** 82% of full-time CISOs report feelings of burnout, 64% are considering quitting
- **Availability:** Better availability than freelance experts, ready to work when you need them

The model of using — and paying for — only the expertise and services you need is gaining popularity in many fields. A vCISO can save your organization money without compromising your information security program's efficacy.



"Could Your Business Benefit From a vCISO?" Read our blog post for more on the benefits of working with a vCISO.

Read Articles

Did You Know?

The US cybersecurity workforce would need to increase by 62% to meet current demand levels.

12. Cyber Forensics Consulting

When most people think of information security risks, they focus on financial losses, operational disruptions and reputational damage. But a data breach can also leave you vulnerable to legal action from clients or partners. Understanding your legal rights and responsibilities is vital to protecting your organization from harm.

If your cybersecurity attorney works with a cyber forensics consultant, they can help shape your information security program with an eye toward your legal obligations and shield you from lawsuits in the event of a breach.

Identify Issues	Oversee Operations	Guide Security Leaders
Pointing out legal strengths and weaknesses in your information security strategy	Ensuring security measures, policies and standards comply with legal obligations	Assisting with governance and incident response efforts with an eye towards legal issues

Get more information on protecting your business from legal liability in this post for attorneys: "Why Your Clients Really Need Cyber Forensics."

Read Articles

Did You Know?

A Gartner survey found that the recent move to remote working during the pandemic increased most cybersecurity leaders' concerns about legal and compliance issues.

13. Avoiding Data Breaches

The goal of your information security strategy is to secure your data against the exposure to unauthorized parties. And threats and vulnerabilities can be everywhere. While the expression "data breach" often conjures up images of remote hackers using code to bypass our security measures, the risks are often more commonplace.

Data breaches can be caused by:

- Employee Error
- Social Engineering
- Visitor Access
- Hackers
- Ransomware
- Disgruntled Staff
- Physical Theft

Organizations of all sizes and verticals can fall prey to breaches that expose the personal or sensitive data of their customers or business-critical information and trade secrets.

AIS Network

We've teamed up with some analysts to examine what caused some major security breaches of 2020 and how they could have been prevented in "What You Need to Know About Avoiding Data Breaches."

Read Articles

Did You Know?

The average cost of a data breach is $3.92 million. But breaches contained within 200 days cost $1.2 million less on average than longer incidents.

Your Information Security Partner

At AISN, we understand the challenges today's businesses face in protecting their systems and data against ever-evolving threats. We've spent over 25 years developing the knowledge, experience and partnerships necessary to help our clients develop and maintain information security programs that protect assets and manage compliance with regulatory and industry requirements.

If you have questions about information security, cybersecurity governance or cyber forensics, we have answers. Our experts are always happy to discuss your needs, so get in touch with us today.

CONTACT US TODAY

AIS Network
919 E. Main Street, Suite 1000, Richmond, VA 23219

www.aisn.net | sales@aisn.net | 888-401-AISN