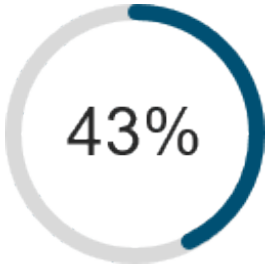
Small Business Security Essentials

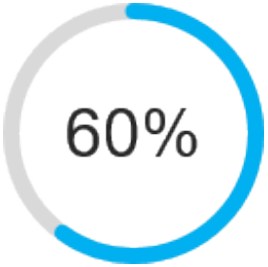
Stay ahead of the game on security

Learn what the Small Business cyber-threat landscape looks like today so your business can survive; reduce operational costs and grow securely; make security a priority for everyone, and protect your business with Cisco.

As your business grows, it gets noticed and not all of the attention is welcome. More and more sophisticated criminal gangs are going after small businesses.



43%
of cyberattacks target small businesses. [1]



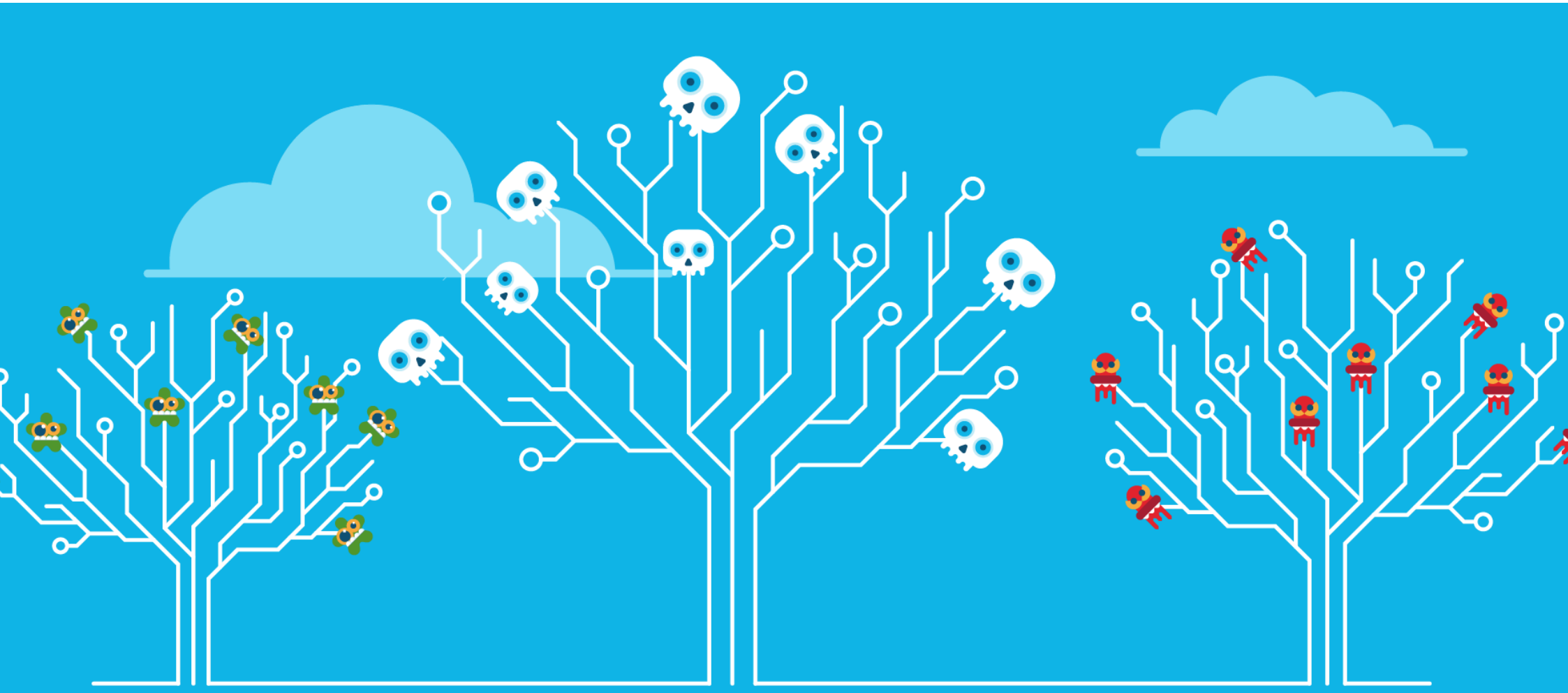
60%
of them will be forced to close as a result. [1]

Cisco Annual Cybersecurity Report 2018 'Cisco ACR 2018'

$2,235,018 per year

The average amount Small Businesses spent in the aftermath of a cyber attack or data breach due to damage or theft of IT assets and disruption to normal operations.

It's a bitter truth that means your business' survival depends on understanding cyber security.



Threats are becoming more sophisticated

Hackers know your weaknesses and how to exploit them

Fewer of today's hackers are in it 'just for fun' or a challenge. Most are money motivated, highly organised and seldom work alone. Attackers are agile, while businesses can't always say the same. Especially when they've just been 'making do' with security.

'A hacker's goal is to steal credit card information, email addresses, usernames and passwords. Anything that can be sold on to a higher bidder. *How* they do it may include some of the following techniques.

Ransomware

Attackers can hold businesses virtually hostage, with ransomware; a ruthless practice. Ransomware remotely encrypts your files without your consent. Some forms of ransomware are programmed to spread across the network.

Instead of requiring a recipient to open an email attachment or click on a link, current trends in ransomware—such as WannaCry, which began in May 2017—enable malicious code to be transmitted between networks without user interaction. "WannaCry is the first one to completely automate," says Craig Williams, a senior security outreach manager at Talos, the security research arm of Cisco.

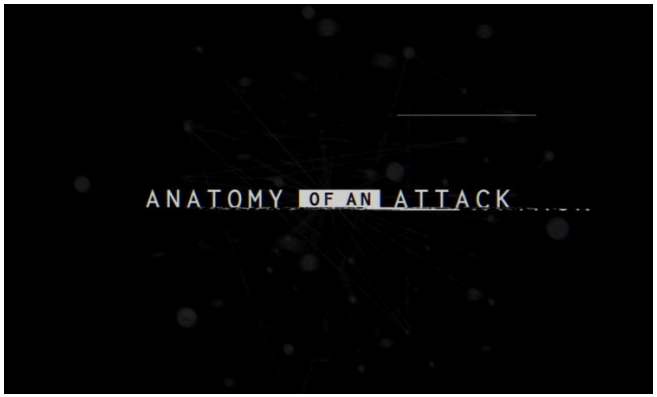
WannaCry affected more than 200,000 computers worldwide, and may cause an estimated $4 billion in losses. WannaCry gets installed through a vulnerability in the Microsoft Small Business protocol and is particularly effective in older Windows environments, such as Windows XP, Windows Server 2003 and Windows 8. Microsoft had already released a security update to patch this vulnerability, but not all users were automatically protected.

Small Businesses held to Ransom

Fifty-two percent of the Small Businesses—participating in the Ponemon Institute's 2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB) report—experienced either a successful or unsuccessful ransomware attack in a 12 month period. Once the infection is complete, a message will appear on your screen, demanding that you pay a ransom in bitcoins for the release of your data. A typical ransom can be anywhere from £200 to £10,000, but some victims have ended up paying a lot more.
Recent headlines show a new generation of threats going viral on a global scale and proliferating more quickly than ever. Cisco Talos threat research group uncovered a threat, called VPNFilter, that compromised more than 500,000 small office/home office routers and network attached storage devices around the world. Cisco devices were not among those affected. This

complex threat allows the actor to inspect traffic that is passing through the devices, to steal files off network backup drives, and potentially pivot onto connected corporate networks.

Cyber criminals understand their targets – down to their likes and dislikes and how they conduct business. They know what they will pay for their data to be released, and they exploit any weakness they find ruthlessly.



Business Email Compromise (BEC)

Business email compromises (BEC) are 75% more profitable than ransomware. Despite that, they don't get as much publicity.

BEC are targeted attacks, in which hackers use social engineering to trick people into transferring money to them. There is no malware, there are no attachments. Unlike ransomware attacks, they don't take any data from their victims. It's all based on lies and misdirection.

Typically, hackers spend some time researching their targeted company and start building a profile. After they know enough, they may send spear phishing emails to senior members of staff, often in the finance department. It needs to be someone with the authority to transfer the money. The bigger the company, the more money they can make. However, attacks targeting small and medium-sized companies are on the increase.

The bigger the company, the more money they can make. However, attacks targeting small and medium-sized companies are on the increase.

Data Breach

Data is at the heart of everything your company does: it's your intellectual property, your next big break, your customer records, your revenue. A breach costs much more than just fixing outages and damaged systems.

Building a strong security posture can help protect your intellectual property and your reputation. On average, it takes organisations 191 days to detect a breach and 66 days to contain it. (Source: Ponemon Institute). Yet the key to damage limitation is early detection.

Cisco's median time-to-detection is 3.5 hours. If a breach happens, Cisco Incident Response Services experts are available within hours to help you contain it and fix the root causes.

Supply chain attacks

Supply chain attacks are an emerging and growing cyber threat, which demonstrates how skilled cyber criminals have become. What happens is that the bad guys compromise the software update mechanisms of (otherwise legitimate) software packages. That then allows them to piggy-back on the distribution of genuine software.

Crucially, the cyber criminals will target a business in the supply chain with weak cyber security practices – especially when it comes to sharing information. This is why small businesses often get targeted.

Once they've identified the weak link, the attacker can then focus on the exploitation of the ultimate, intended target.

Defend vs attackers everywhere

Don't let attackers sidetrack your business. Fight them at all the places where they try to get in. Our solutions protect you from the DNS layer to email to the endpoint. And they are backed by industry-leading Talos threat research.

What to do

If you have a place in a supply chain, ask your vendors/partners how they secure their supply chains. Ask them about their development practices and their internal security controls. How do they roll out patches and updates to their internal systems, and how often? How do they segment and secure their development, QA, and production environments? How do they vet their partners and vendors?

And be sure to ask all of these questions of your own organisation, or you could find that it's your organisation that is the weakest link in the supply chain.

More info about supply chain attacks:
https://gblogs.cisco.com/uki/protecting-against-supply-chain-attacks/

Too many businesses have a ‘stacking problem’

Some businesses just don’t have a clear cyber security strategy. They make do with a solution until it becomes a hindrance.

Others attempt to cover all bases and end up with a stacking problem. A stack of various point security solutions from different vendors, all in place at once. Both situations spell trouble.

The patchwork of incompatible security technology leaves gaps, creates management headaches and makes inefficiencies upon which hackers thrive. Each new security solution comes with another management interface. Each new solution demands human resources, management hours to set up, set policy, respond to alerts and it’s not always clear whether the extra security outcome you gain is worth all the extra effort you are putting into managing that solution – rather than focusing on bigger problems elsewhere.

You may have added complexity without much overall incremental effectiveness. This situation isn’t helped by the fact that security is still seen as primarily an ‘IT issue’. According to the Cisco Security Benchmarks Study, some organisations don’t particularly agree that line of business managers are engaged with security. The attitude is too often, ‘Security is IT’s problem.’ This is a real issue, because it means that security often gets ‘bolted on’ rather than embedded in a company’s ecosystem. Cutting corners creates more work.

Done right, security can be a business enabler. A platform for growth.

The ‘attack surface' is getting larger, and more complicated

We work everywhere: at home, in the office, airports, coffee shops. Yet traditional security solutions still focus on protecting employees only while on the business network.

Picture the scene:

- Users are accessing your network from their own smart devices, from wherever they are

- Your business apps, servers, and data are in the cloud

- Devices that don't even look like computers are connecting to your networks (think smart meters, thermostats, printers, cameras...)

- And to thicken the plot, you need to figure out how to get security everywhere to secure this complex infrastructure

Shadow IT

Shadow IT is the practice of employees using any applications they fancy, without getting the IT department's approval. This can be anything from installing an instant messenger service onto a work device, to downloading their own file sharing software and using it to transfer sensitive data.

Of the respondents participating in the Ponemon Institute's 2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB) report that experienced a data breach, 54 percent say negligent employees were the root cause—an increase from 48 percent of respondents in the previous year's study.

Shadow IT can create huge security vulnerabilities, especially if you don't know how far the problem extends. This kind of operation is like going for a swim in shark-infested waters wearing a meat suit. Yet it's incredibly prevalent in businesses. So why does it happen?

In fairness to staff, it happens with best intentions. Workers want to improve their own levels of productivity and use the latest digital tools. Staff are not usually thinking about the security implications when accessing these applications. Sometimes, employees use Shadow IT tools because they were used to certain systems in their previous organisation. After all, it's easier than learning something new.

Shine a light on Shadow IT

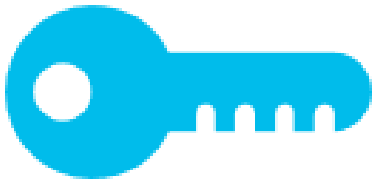
It's possible to turn shadow IT into a positive contribution to your business:

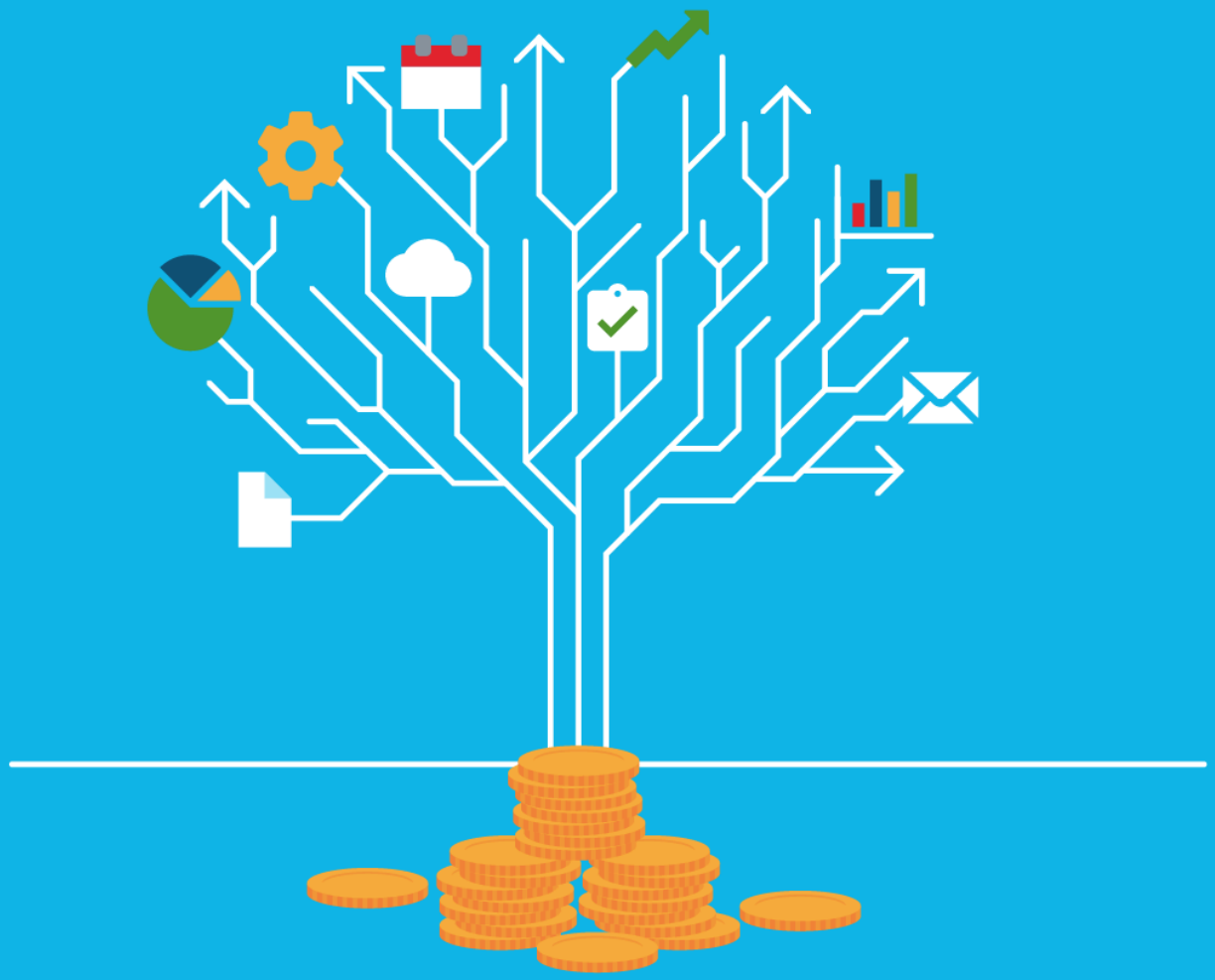
- If you don't already, set up a forum or an 'ideas on a postcard' tool that allows your employees to submit ideas that could improve the running of the business. Reward people for doing this, and celebrate when an idea becomes reality.
- Effective security isn't just about the technology – it's also about setting the right processes. Make security awareness a fundamental part of your training programme, so that people understand the consequences of using insecure devices and programmes.
- Knowing what's happening in your network is a huge priority in IT security. Unfortunately, most businesses don't know when a breach has taken place, how it got in, or how bad the damage is. Reverse that.

Password Policy

Robust passwords continue to play an essential role in small busines cybersecurity. Yet 59 percent of respondents in the current Ponemon report–the same percentage as the previous report–say they do not have visibility into employee password practices, including the use of unique or strong passwords.

Respondents also say that password policies are not strictly enforced. If a company has a password policy (43 percent of respondents do), 68 percent say it is either not strictly enforced or they are unsure how well it is administered.





Growth requires security

Cyber Weakness Hurts Innovation

Deflecting cyberattacks is certainly a pressing concern, but a more troubling outcome of weak cybersecurity is its impact on company growth and innovation.

In a recent study by Cisco, a stunning 71 percent of executives said concerns over cybersecurity had impeded innovation at their companies. Among respondents, 39 percent said they had halted mission-critical initiatives due to cybersecurity issues. These responses highlight how cybersecurity weakness impedes the ability of firms to innovate at precisely the time they need to do so to compete.

Digitisation, disruption, and exponential change have become the new normal of an intensely competitive business environment. Nimble businesses can establish a clear lead over the competition if they can innovate, move quickly, and reward experimentation.

A Breach Impacts More Than the Bottom Line

Failing to secure your network can have far-reaching consequences, including: downtime, equipment damage and replacement, incident response, forensic investigation, internal audits and communications.

A loss of customer confidence can permanently damage a previously strong revenue stream. Losing your customers' data may result in legal action, fines, increased regulation and remediation costs. Yet the damage does not stop there. For example, if a retailer suffers a data breach, customers may not feel comfortable sharing personal information anymore.

Your business can gain a decisive advantage by harnessing:

- Established technologies such the web, mobile, cloud, enterprise resource management, and customer relationship management

- Fast developing technologies like artificial intelligence and data analytics

These technologies help businesses better connect with their customers, reach new markets, and enhance worker productivity, while also boosting revenues and cutting costs. Cybersecurity concerns can hinder the pursuit of some digital business models and innovations.

Damned if you do and damned if you don't

Many business people have a bad choice. A risk of getting it wrong or a risk of getting left behind. They feel they must continue to press forward or

They feel they must continue to press forward or risk being overtaken by digital disruptors and other agile competitors. In our survey, 73 percent of respondents admitted they often embraced new technologies and business processes, despite the cybersecurity risk.

Sub-par cybersecurity leaves businesses in the worst possible competitive position: not innovating fast enough to compete, yet not safe enough from cyber attack, despite delaying digital innovations.

How would a security breach or a ransomware attack affect your business?

What is the potential financial impact of a network outage due to a security breach, or loss of access to data and systems due to a ransomware attack?

- Could a security breach or ransomware attack disrupt your supply chain?
- What would happen if an attack caused your website to go down?
- Does your company rely on e-commerce features on its website?
- How long could the site be down before your business lost money?
- Is your company insured against cyber attacks, or against the misuse of your customers' data? Is this insurance adequate?
- Does your company have backup and recovery capabilities to restore information, if necessary, after a security breach or loss of data due to a ransomware attack?

Digital Value at Stake

Digital Value at Stake is a way to place a value on security. It is based on entirely new sources of value emanating from digital investments and innovation, and value shifting among companies based on their ability to harness digital capabilities.

Part of the Digital Value at Stake comes from the defensive side of cybersecurity, such as:

- Protection of intellectual property
- Reduction of compromised data (both internal and customer information) Increased business uptime and reduced network downtime
- Protection of financial assets
- Safeguarding of sensitive government, national, and political information
- Preservation of business reputation

Get the full picture. Read Cisco's Ultimate Guide to Cybersecurity to Drive Profitability.

A secure platform for growth

Cisco's integrated security architecture helps businesses: to improve security effectiveness by minimising the time to detect threats and resolve incidents, to drive savings (in both capital outlay and operational expenditure) and improve IT staff productivity.

Getting everyone on board with cybersecurity

Make security a priority for everybody

Sometimes it takes a big hit for everybody to get on board with cybersecurity initiatives.

60% of small businesses who suffer a cybersecurity breach are forced to close. Which means, for you especially, prevention is better than cure.

Present the risk factors specific to your company

Help your board understand the security threats that could affect your particular organisation. Don't spend too much time presenting generic trends and statistics. Instead, help them see the connection between those security trends and the challenges that are very specific to your business and industry. The more context you can provide, the more relevant it will be to your board.

For example, you can talk to them about your company's biggest source of revenue and give them examples of how security threats such as ransomware could pose a threat. If your company keeps sensitive data such as financial records, you could you show examples of the legal implications and fines your organisation could incur if such data was publicly released.

Show them how an attack works, how easy it can be to compromise security. Give them real examples of the issues you are already facing as well as the risks and the long-term effects that those problems could have.

Quantify everything

Executives like their metrics and numbers. It is, therefore, important that you align your security priorities to your company's goals and deadlines. Acknowledge their business and IT priorities and show how security will help them achieve it.

Show also the flip side: how a security incident could put their plans at risk. For example, if you are about to launch a new product, what is the potential damage to your business of having that intellectual property made public or destroyed?

In fact, it doesn't need to be a hypothetical issue. If you can quantify how existing security issues are already costing your business, then that makes for an even better argument.

Repeat, repeat, repeat

It is unlikely that you will get everything you need from a one-off conversation. Make your communication simple and frequent. Establish regular catch-ups and report often on relevant metrics. Don't be afraid to repeat yourself and try out a few different angles until the message gets across and you secure the funds and support you need.

How GDPR will help

In many cases, security professionals struggle to speak the same language as their board of executives and help them understand why they need to prioritise investment in security. When a public cyber attack happens and executives see the multidimensional damage it causes, then those reasons to invest become crystal clear. Conversations (and changes) happen at a much faster pace when everyone understands the issue.

This is where laws such as the General Data Protection Regulation (GDPR), which took effect in May 2018, can help improve security.

Companies that are already investing in security may not have a lot to worry about, as they are probably well on the way to being compliant (on the security side of GDPR). On the other hand, for those organisations that have been struggling to secure funds to invest, GDPR offers a great opportunity to get security professionals and top leaders on the same page. New legislations such as this are forcing minimum standards on companies, which will help support greater technology innovation in the future.

Data privacy and IT security are not only regulatory requirements, but also customer demands. It is becoming more frequent for companies to get questions from their customers about how they are handling their data. There is a relationship of trust, an assumption that the company receiving their data will take good care of it. The law is just there to ensure that companies are doing all they can to honour that trust.

Protect your business with Cisco

Network Security

What is Network Security?

Network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network.

How does network security work?

Network security combines multiple layers of defenses at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats.

How do I benefit from network security?

Digitization has transformed our world, how we live, work, play, and learn. Every organization that wants to deliver the services that customers and employees demand must protect its network, and its proprietary information from attack. Ultimately it protects your reputation.

6 steps you can take to secure your network

1. Monitor the traffic coming in and going out your firewall and read the reports carefully. Don't rely on alerts to flag dangerous activity. Make sure someone on your team understands the data and is prepared to take the necessary action.
2. Keep an eye on new threats as they're discovered and posted online. For example, the Cisco Talos blog provides instant updates on new threats, vulnerabilities and a detailed weekly threat roundup. Trend Micro's TrendWatch site tracks current threat activity. Also, you can have the U.S. Computer Emergency Readiness Team (US-CERT, a division of Homeland Security) email alerts to you about recently confirmed software vulnerabilities and exploits.
3. Enable regular updates for your firewall and anti-virus software.
4. Train employees on an ongoing basis so they understand any changes to your acceptable-use policy. Also, encourage a "neighborhood watch" approach to security. If an employee notices anything suspicious, such as not being able to log into an email account right away, he or she should notify the appropriate person immediately.
5. Install a data protection solution. This type of device can protect your business from data loss if your network's security is breached.
6. Consider additional security solutions that will further protect your network as well as expand your company's capabilities.

Types of Network Security

Access control

Not every user should have access to your network.To keep out potential attackers, you need to recognize each user and each device. Then you can enforce your security policies. You can block noncompliant endpoint devices or give them only limited access. This process is network access control (NAC).

Application security

Any software you use to run your business needs to be protected, whether your IT staff builds it or whether you buy it. Unfortunately, any application may contain holes, or vulnerabilities, that attackers can use to infiltrate your network. Application security encompasses the hardware, software, and processes you use to close those holes.

Antivirus and antimalware software

“Malware,” short for “malicious software,” includes viruses, worms, Trojans, ransomware, and spyware. Sometimes malware will infect a network but lie dormant for days or even weeks. The best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.

Data loss prevention

Organizations must make sure that their staff does not send sensitive information outside the network. Data loss prevention, or DLP, technologies can stop people from uploading, forwarding, or even printing critical information in an unsafe manner.

Behavioral analytics

To detect abnormal network behavior, you must know what normal behavior looks like. Behavioral analytics tools automatically discern activities that deviate from the norm. Your security team can then better identify indicators of compromise that pose a potential problem and quickly remediate threats.

Email security

Email gateways are the number one threat vector for a security breach. Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send them to sites serving up malware. An email security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data.

Firewalls

Firewalls put up a barrier between your trusted internal network and untrusted outside networks, such as the Internet. They use a set of defined rules to allow or block traffic. A firewall can be

hardware, software, or both. Cisco offers unified threat management (UTM) devices and threat-focused next-generation firewalls.

Intrusion prevention systems

An intrusion prevention system (IPS) scans network traffic to actively block attacks. Cisco Next-Generation IPS (NGIPS) appliances do this by correlating huge amounts of global threat intelligence to not only block malicious activity but also track the progression of suspect files and malware across the network to prevent the spread of outbreaks and reinfection.

Mobile device security

Cybercriminals are increasingly targeting mobile devices and apps. Within the next 3 years, 90 percent of IT organizations may support corporate applications on personal mobile devices. Of course, you need to control which devices can access your network. You will also need to configure their connections to keep network traffic private.

Network segmentation

Software-defined segmentation puts network traffic into different classifications and makes enforcing security policies easier. Ideally, the classifications are based on endpoint identity, not mere IP addresses. You can assign access rights based on role, location, and more so that the right level of access is given to the right people and suspicious devices are contained and remediated.

VPN

A virtual private network encrypts the connection from an endpoint to a network, often over the internet. Typically, a remote-access VPN uses IPsec or Secure Sockets Layer to authenticate the communication between device and network.

Web security

A web security solution will control your staff's web use, block web-based threats, and deny access to malicious websites. It will protect your web gateway on site or in the cloud. "Web security" also refers to the steps you take to protect your own website.

Wireless security

Wireless networks are not as secure as wired ones. Without stringent security measures, installing a wireless LAN can be like putting Ethernet ports everywhere, including the parking lot. To prevent an exploit from taking hold, you need products specifically designed to protect a wireless network.

Talos Threat Intelligence

Talos is Cisco's industry-leading threat research and intelligence team, and every Cisco security product is protected through Talos. Talos has more than 250 threat researchers working round the clock and across the globe, with a repository of

100 terabytes of threat intelligence.

We see a third of the world's email traffic daily and over 2 percent of the world's DNS requests. We encounter over 1.1 million unique malware samples each day through our Advanced Malware Protection (AMP) and threatGRID technology, which allows us to block 19.7 billion threats a day on our customers' networks.

That's right–19.7 billion threats blocked a day.

Such vast knowledge and research capabilities underwrite Cisco's cybersecurity solutions, which offer the visibility, automation, flexibility, and scalability required to protect your network environment against increasingly sophisticated threats.

Cisco Umbrella

A cloud security service that provides built-in protection for your internet service

Cisco Umbrella is a cloud security service that provides built-in protection against attacks over your internet connection, helping you mitigate the time and cost spent dealing with cyber attacks.

The solution provides proactive protection against threats on the internet, such as malware, botnets and phishing attacks. It helps keep your business safe by delivering clean traffic before it reaches your internal network, effectively learning where attacks are being staged, and blocking threats over all ports and protocols. You can be confident that with secure internet access, you are protected with a first layer of defence against malware.

Cisco Umbrella provides visibility into all internet requests across your network, across every port, protocol or app to uncover and block connections to malicious domains and IP's. See why small businesses are realizing the security multiplier effect by using DNS to complement existing security measures. What attacks aren't you seeing?

Next Generation Firewall

A traditional firewall is able to control the traffic at the point of entry or exit within the network. In other words, it's the drawbridge between your own business and the 'great unwashed' of the rest of the internet.

This was perfect for those simple times – back when you used to be able to see everything that was latching onto your network. Now, businesses are increasingly playing host to a myriad of unknown devices, and a deep dark sea of cloud applications which are downloaded by employees.

The main difference with a next generation firewall is that you can set application controls and policies. For example, if a member of your staff downloads some file sharing software that may be unsecure, this will be automatically be made visible and you can do something about it instantly.

Plus, overall you will gain far more visibility and control over the users, devices, threats, and vulnerabilities in your network. So when your board asks you, “Are we secure?” you can provide a much more comprehensive answer than if you have a traditional firewall that only controls traffic.

Learn more about Next Generation Firewalls or find the best Next Generation Firewall for you.

Advanced Malware Protection

Next-generation endpoint security

Next-generation endpoint security is the integration of prevention, detection, and response capabilities in a single solution, leveraging the power of cloud-based analytics. Cisco AMP for Endpoints is a lightweight connector that works on your Windows, Mac, Linux, Android, and iOS devices.

Cisco AMP for Endpoints provides comprehensive protection against the most advanced attacks. It prevents breaches and blocks malware at the point of entry, then rapidly detects, contains, and remediates advanced threats that evade front-line defenses and get inside your network.

Prevent: Strengthen defences using the best global threat intelligence, and block both fileless and file-based malware in real time.

Detect: Continuously monitor and record all file activity to quickly detect stealthy malware.

Respond: Accelerate investigations and automatically remediate malware across PCs, Macs, Linux, servers, and mobile devices (Android and iOS).

It can use the public cloud or be deployed as a private cloud. AMP continuously monitors and analyzes all file and process activity within your network to uncover the 1 percent of threats that other solutions miss. AMP never loses sight of where a file goes or what it does. If a file that appeared clean upon initial inspection ever exhibits malicious behavior, AMP is there with a full history of the threat’s behavior to catch, contain, and remediate.

Discover Unknown Threats

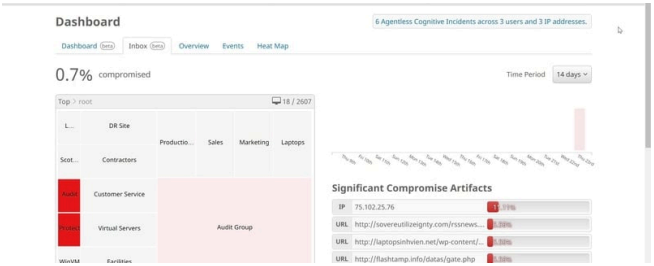
AMP's built-in sandboxing technology analyzes the behavior of suspicious files and correlates it against other information sources. File analysis produces detailed information to give you a better understanding of how to contain the outbreak and block future attacks.

When a file is deemed malicious, AMP drastically reduces the amount of time and resources required to investigate. It automatically provides insight into your most pressing questions, including:

- What happened?
- Where did the malware come from?
- Where has the malware been?
- What is the malware doing now?
- How do we stop it?

With a few clicks in AMP's browser-based management console, the file can be blocked from running on all endpoints. Cisco AMP knows every other endpoint the file has reached, so it can quarantine the file for all users. With AMP, malware remediation is surgical, with no associated collateral damage to IT systems or the business.

How to Stop and Quarantine a File with Cisco AMP:



Cisco Meraki

Cloud Managed Security & SD-WAN

100% centralized cloud management for security, networking, and application control.

Cisco Meraki Security Appliances can be remotely deployed in minutes using zero-touch cloud provisioning. Security settings are simple to synchronize across thousands of sites using templates. Auto VPN technology securely connects branches in 3 clicks, through an intuitive, web-based dashboard.

Comprehensive Security in a Single Box

Every Meraki Security Appliance supports several features, like a stateful firewall and integrated Sourcefire intrusion prevention (IPS) engine, to keep networks secure. Threat definitions and filter lists are seamlessly updated, ensuring every site has bleeding-edge protection from the latest vulnerabilities and troublesome websites.

Secure a Site in Minutes

1. Add Meraki Security Appliance to dashboard.
2. Enable intrusion prevention.
3. Select desired threat protection level.

Find out more

For the latest insight and innovation, visit: Cisco Tech Connection for Small Business or explore more Cisco Small Business resources and Cisco Security to protect your business.

Thank you for reading

Small Business Security Essentials