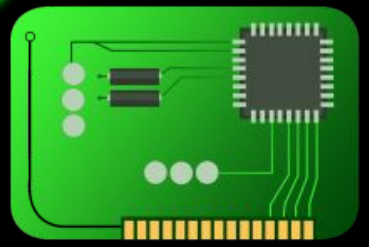
Computer Guts



Taking Control of Your Cybersecurity

What is cybercrime?

1. Common misconceptions
2. Why should you care?
3. Take control of your cybersecurity
4. Assess risk with CIS

What is cybercrime?

Cybercrime is a broad range of malicious activity from cyberbullying to worms and viruses, but it also includes:

- Illicit and/or illegal online markets
- Trade secrets and/or IP theft
- Crimeware, CaaS (Crimeware-as-a-service)
- Ransomware

Common Misconceptions

As reflected by what SMBs are saying

“It’s too expensive to protect ourselves.”

“An attack/breach won’t happen to us.”

“Our data is in the cloud, so it’s safe, right?”

“We’re too small to be targeted.”

“We don’t have anything hackers want.”

“...a data breach could well be fatal and end an SMB’s business, while others remain unaware of the catastrophic potential, according to a new survey on cyberattacks and their impact on American businesses with employees numbering from 1-9 up to 200-250 per organization.”

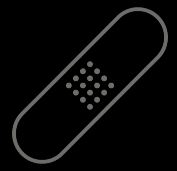
Roger Aitken, Forbes

Source: Forbes, Cybercrime & Hackers 'More Devastating' To SMB's Than Fire, Flood & Transit Strike Combined

Why should you care about cybercrime?

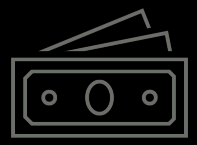
Victims of cyberattacks experience a variety of losses:

Customer protection

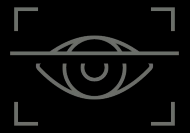


Career damage

Company reputation



Financial cost



Product protection

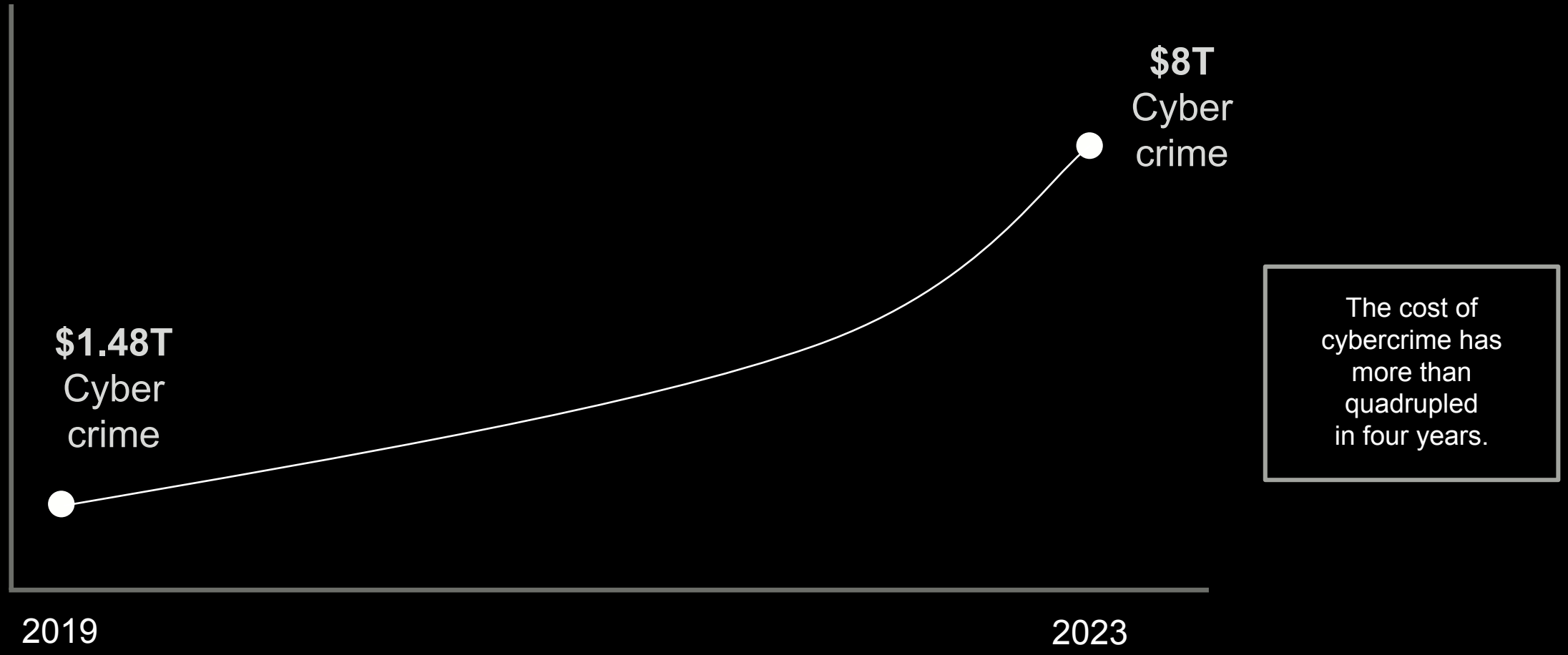
It’s about risk tolerance

You need to balance the answers to these two questions:

- How much are you willing to accept?
- How much are you willing to pay to mitigate?

The cost for inaction may be more than you realize…

Cybercrime’s exponential growth



The cost of cybercrime has more than quadrupled in four years.

Source: Mimecast

Assume breach

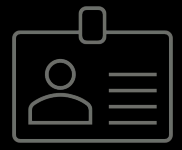
- Assume a breach since no system is unbreachable
- Have a sense of inevitability around having an incident
- Maintain hope! The proper measures can mitigate risk

What can you do?

1. Take all reasonable measures to keep the bad guys out
2. If you are breached, limit the impact:
    - How do you segment off and protect your most valuable assets?
    - How do you limit the "blast radius" of a breach?
    - How do you identify the threat actors that have successfully breached your environment and just haven't made themselves known yet?

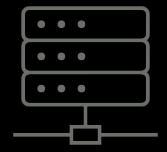
Don’t be a victim

Modern companies need to become digital fortresses with multiple layers of proactive protection that serve to monitor, detect, alert, and prevent the onslaught of cyberattacks.



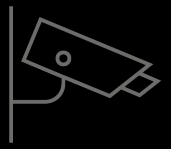
Identity protections and access management

Remote monitoring and SOC



Backup and disaster recovery

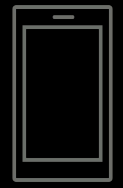
Email security



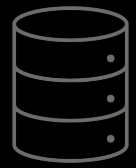
Web and network security

End user training

Endpoint security



Mobile security



Data protection

Real-life stories:

A $250,000 breach for a small mortgage company

The setup:

A small mortgage company, about 25-30 employees, had been engaging in regular closings with a law firm. One day they receive an email saying, “Please wire the money to this new account.” Accounting thought it seemed weird, but the email address looked correct, so they wired the money.

What happened behind the scenes:

The threat actors compromised their email months ago, successfully phishing credentials and passwords. They then saw that one of the law firms they had successfully breached used a lowercase L in its name. So, the threat actors purchased the same domain, but used a capital L instead of a lowercase one. Accounting received the email request and didn't spot the capital letter in place of its correct lowercase counterpart. As a result, they wired $250,000 to escrow and within seconds, it was disseminated to 100 different accounts all over the world. Untraceable.

The result:

The mortgage company didn't have cybersecurity insurance. The owner of the company had to write a $250,000 check out of his home equity line to keep the business afloat.

Real-life stories:

Supply chain attack at private school

The setup:

A private school with limited resources had everyone complaining about variations in temperatures in campus buildings. They bought 10 smart thermostats online so the administrator could control the temperatures remotely. They didn't realize the smart thermostats were programmed to have an open connection to the cloud to get updates via Wi-Fi.

What happened behind the scenes:

Threat actors identified the cheap smart thermostats online and knew they were constantly looking for updates. They pushed what looked like an update but was actually malicious code that successfully breached the school's network and landed them behind the firewall. They quickly installed ransomware, encrypted the school's files, deleted the backups, and requested payment.

The result:

Because they had no backups, the school had to pay the ransom from funds that were supposed to power normal operations. They finally got the ransom keys from the threat actors and had to de-encrypt all their files, losing a good portion in the process due to the files being corrupted.

Direct assaults

Password attacks

DDoS attacks

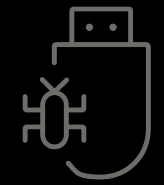
SMB

Sneak attacks

Trojan horses

Spyware and eavesdropping

Phishing



Malware, worms, and viruses

Ransomware

What is CIS?

Center for Internet Security

Nonprofit organization established in 2008

Endorsed by PCI, HIPAA, FedRAMP, NIST, and cyber insurance agencies

Adopted by 170,000 organizations and 27% of top MSPs (Source: Datto) - Including Computer Guts

Resources and benefits

- CIS benchmarks
- CIS hardened images
- Compliance mapping
- Continuous audit and assessment
- A security roadmap

What are the 18 Controls?

18 control families

---

3 implementation groups

---

153 safeguards

Assess Your Risk

CIS readiness process

Begin CIS readiness discovery

Step 1:
Conduct a 1:1 review of the business challenges and CIS benefits.

Step 2:
Review the 18 CIS Controls with a certified security consultant from Computer Guts.

Continue with the CIS assessment

Start implementing CIS Controls internally and externally.

Tooling

Review current tooling strategy, discuss controls alignment, and how Computer Guts can augment.

Enroll in Academy

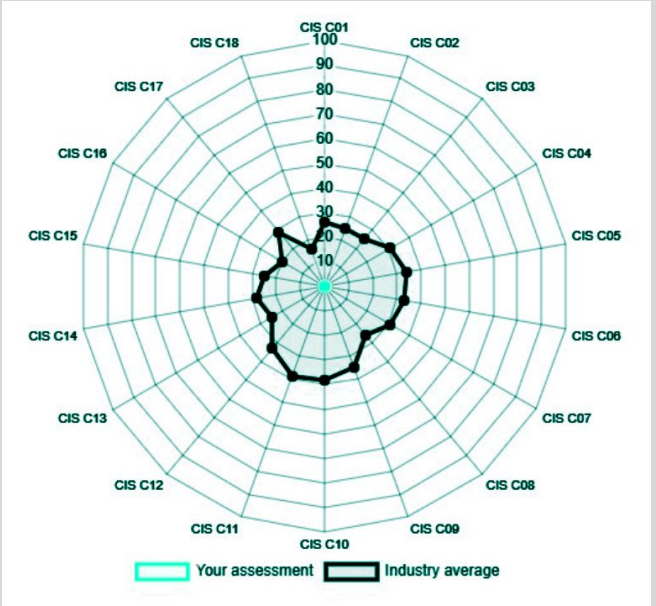
Get your staff ready for CIS assessments. Computer Guts will help get your team started with fundamentals and applying policies.

Own, know, and document your wins

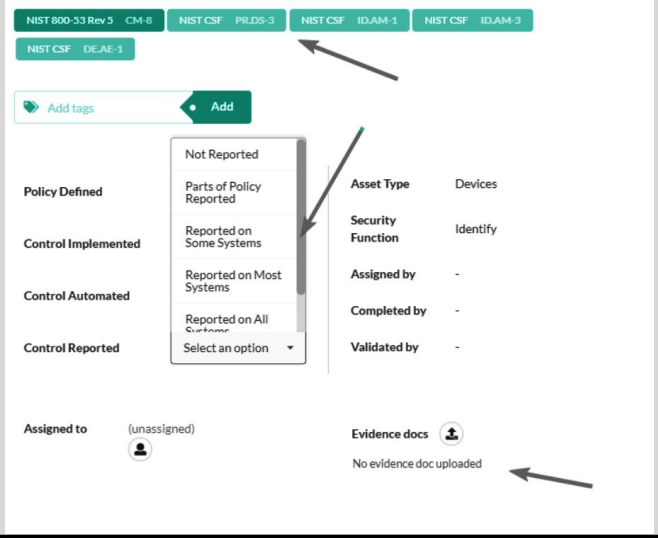
The CIS Controls Self-Assessment Tool, or CIS CSAT, enables security leaders to track and prioritize the implementation of the CIS Controls.

- Create an account to gain access to the free tool
- Take the evaluation
- Honestly use the evaluation to grade your organization and where it stands today

Progress towards alignment



Depth of tool



I have my results. Now what?

Building a Plan of Action and Milestones (PoAM)

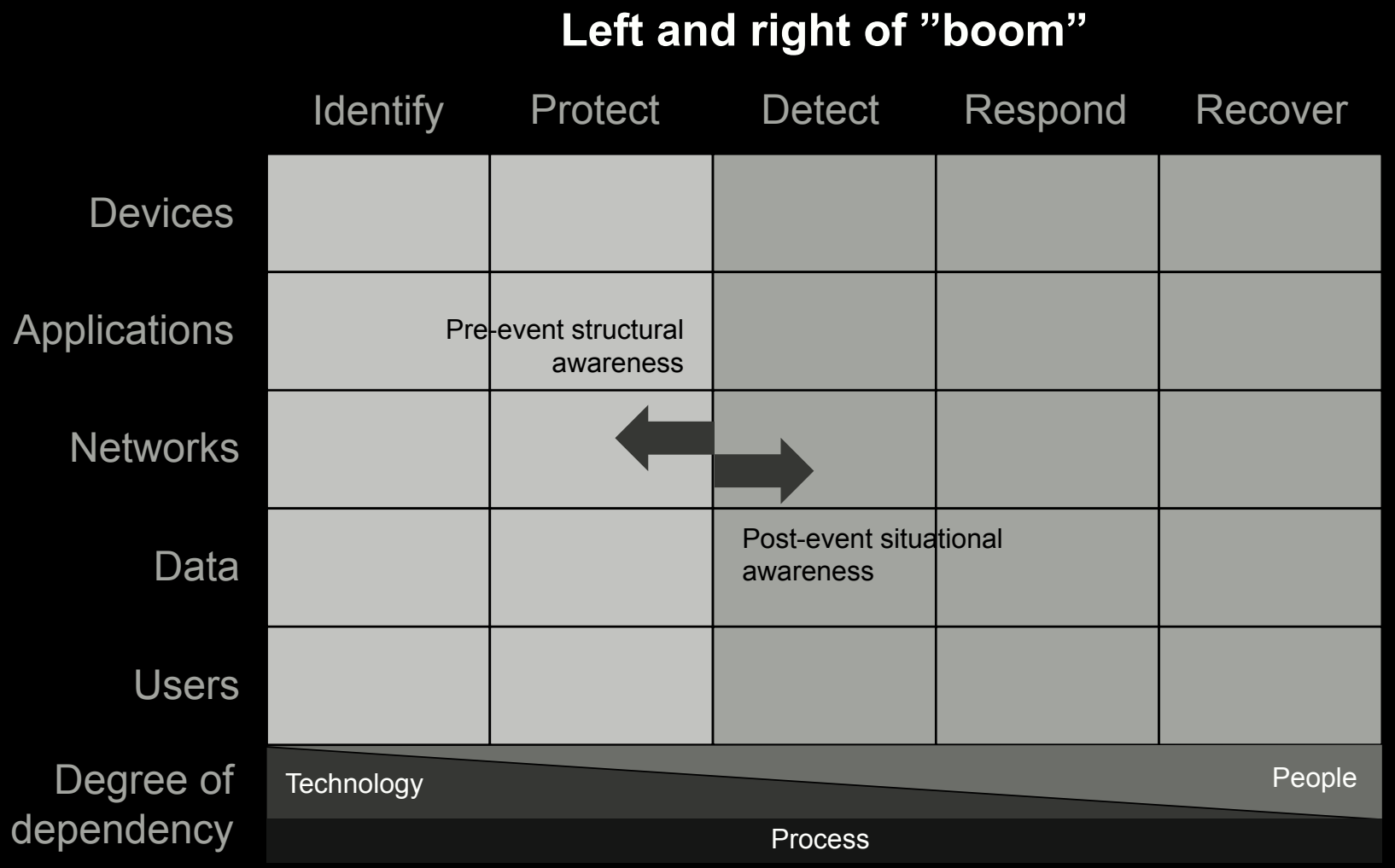
PoAM – Plan of Action and Milestones	Control(s) affected	Priority (1-10)	Milestones of continued effort	Systems affected on BIA
Can implement immediately and easily				
Add MFA to RMM for every account	5.2, 6.3, 6.5	1	Implementing an IDP, ensuring MFA is enforced on condition	Labtech, RMM, IDP (Microsoft)

Your project plan for success

- Look at your risk by magnitude and probability
- Sort by magnitude of effort required for the outcome
- Take small efforts that drive big wins
- Document improvements in policy and project progress

Cyber Defense Matrix

The cyber defense matrix is composed of five assets and five functions. “Boom” is the breach.



Cyber Defense Matrix

Identify	Protect	Detect	Respond	Recover
Inventorying assets and vulnerabilities, measuring attack surface, prioritizing, baselining normal, threat modeling, risk assessment	Preventing or limiting impact, patching, containing, isolating, hardening, managing access ,vulnerability mitigation	Discovering events, triggering on anomalies, hunting for intrusions, security analytics	Acting on events, eradicating intrusion, assessing damage, forensic reconstruction	Returning to normal operations, restoring services, documenting lessons learned, resiliency
Devices	**Apps**	**Networks**	**Data**	**Users**
Workstations, servers, phones, tablets, storage, network devices, IoT infrastructure, etc.	Software, interactions, and application flows on the devices	Connections and traffic flowing among devices and apps, communication paths	Content at rest, in transit, or in use by devices, apps, and networks	The people using the resources on devices, apps, and networks

Remote work is here to stay

Increased remote work means an increase in vulnerability

- Embracing a remote/hybrid work environment means collaboration tools are becoming a new gateway for attacks
- Software suites and their add-ons, such as Microsoft Teams and Slack, put employees' phones, laptops, etc. at a greater risk

Source: Mimecast

The key is protecting mobility

82% of companies are using more of these platforms and **38%** say that the number of attacks due to collaboration tools is on the upswing.

72% of respondents say it is likely, extremely likely, or even inevitable that their organization will be negatively impacted by a collaboration-to ol-based attack in 2023.

75% of respondents believe that collaboration tools pose new threats and create new security loopholes that urgently need to be addressed.

This sentiment was even stronger among respondents at companies where the use of these tools significantly increased during the past 12 months **(82%).**

Source: Mimecast

Datto 2019 State of the Channel Ransomware Report

The cost of cyber threats

Globally, the average cost of a data breach is **$4.45 million.** The average cost in the U.S. is more than double that, at **$9.48 million.**

There was an 84**% rise in ransomware in 2023.**

On average, it takes **204 days** to detect a data breach and another **73 days** to contain it.

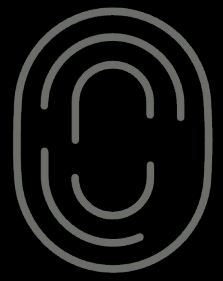
46% of all breaches involved SMB victims.

33 billion electronic records are expected to be stolen.

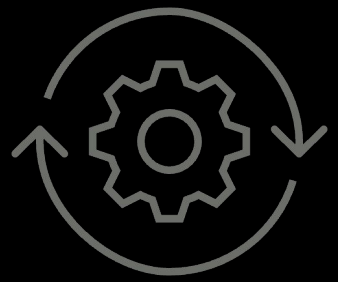
Source: Mimecast

Accenture Cybercrime Study

Four steps you can take right now



Multi-factor authentication (MFA)



Cyber insurance

Password manager

Backup Office 365 & Google Workspace

Take control with a “work from anywhere” security stack

Layer
Anti-virus and EDR
Anti-spam
Anti-phishing
Multi-factor authentication
DNS protection
Security awareness training
Password management
24/7 monitoring (SOC)
Mobile device management

Mobile Security

Summary

In the bring-your-own-device (BYOD) age, protecting smartphones, tablets, laptops, and other portable computing devices, and the networks they connect to, from threats and vulnerabilities is more important than ever. Companies can selectively lock, locate, and wipe devices safely with containerization and protect businesses from mobile cyberattacks.

Benefits

- Simplifies the management and security of smartphones, tablets, laptops, wearables, and IoT
- Scales quickly without compromising security, privacy, or risk levels
- Supports industry and global compliance standards

Endpoint Security

Summary

Protect your various endpoints on a network through cloud-based endpoint security solutions. These endpoints may include mobile devices, laptops, desktops, and servers.

Benefits

- Protects users and business networks from a wide range of threats
- Always up-to-date cloud-based service
- Enables endpoint management anywhere, anytime, online with hierarchical controls and visibility

What is the impact of downtime?

When it comes to ransomware attacks, MSPs report the cost of downtime is

50X

greater than the ransom requested

Average cost of downtime is

$126,000

including lost revenue

Source: https://www.netapp.com/blog/ransomware-cost/

2022 Datto SMB Cybersecurity for MSPs Report

How do you validate your cyber insurance premium spend?

Of the organizations that experienced a ransomware incident, 71% said they paid at least a portion of the demanded ransom.

And while nearly all respondents had cyber insurance, this didn't guarantee that all costs would be covered, or data restored. In fact, only 35% of those affected by ransomware recovered all their data after the incident.

Source: Fortinet, The 2023 Global Ransomware Report

Email Security

Summary

These solutions protect against the most common vector of threats to businesses, which includes spam, phishing, emailed malware, encrypted communications, and more. The right solutions can help protect your business before anything malicious even gets into the network.

Benefits

- Increases employee productivity, while reducing the risk of security breaches
- Enables enforcement of acceptable usage policies and encryption
- Delivers predictable costs and reduces total cost of ownership

Security Training

Summary

These solutions are designed to educate employees about computer security. Even when all other layers of security are planned for and implemented, humans and their behaviors are the weak link. These solutions educate the workforce through fake phishing campaigns, videos, and tips to remain secure.

Benefits

- Strengthens overall internal security
- Boosts security knowledge and awareness for all users
- Identifies high risk employees within an organization

Web Security

Summary

This solution prevents and protects users against web-based threats and provides an enforcement of acceptable use policies to prevent productivity drains.

Benefits

- Prevents web-based threats from infecting the network
- Ensures all web content (including PDFs and resource files) are free from malicious code before it is delivered to users
- Boosts user productivity, ensures compliance, and saves bandwidth by blocking users from visiting inappropriate websites or downloading resource files

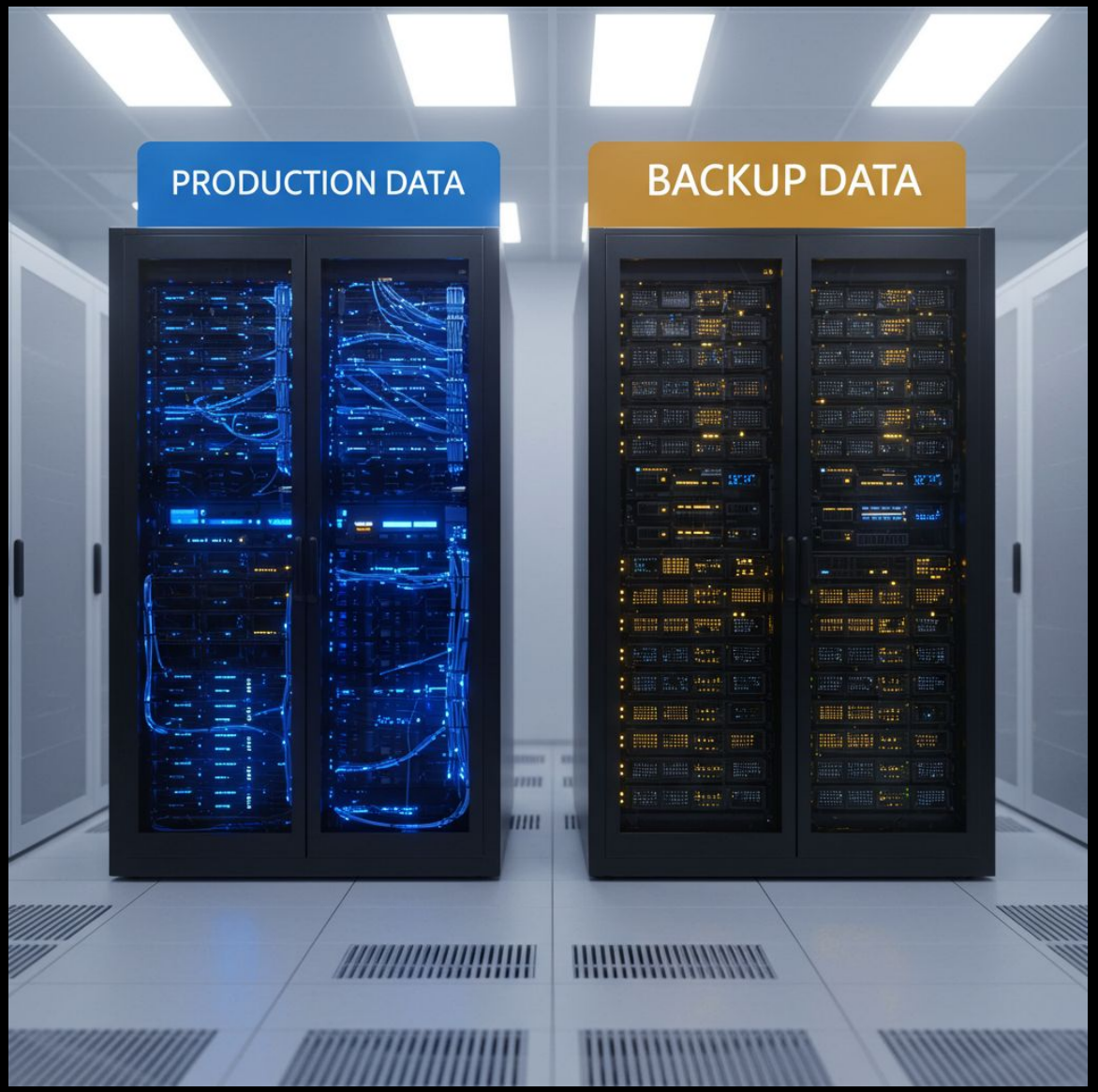
Data Security

Summary

Protect and control your organization's most sensitive data through the utilization of data loss prevention (DLP), as well as file and email encryption, to appease and comply with compliances (HIPAA, CIJS, PCI, etc.).

Benefits

- Helps prevent data breaches and the large costs incurred from litigation
- More secure access to company resources
- Safe sharing of sensitive information inside and outside the organization



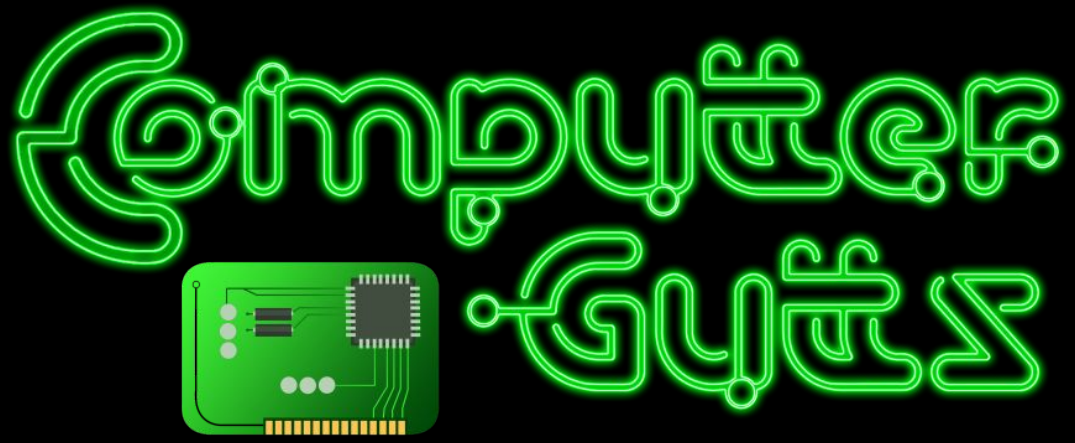
Managed Security

Summary

Today’s cybercriminals have adopted automation, enabling them to go after the SMB market more cost-effectively. To protect our clients, there's a greater need to outsource advanced security to industry experts. Outsourcing security operations enables us to provide 24x7 security monitoring and incident response to protect you from today's advanced threats.

Benefits

- Provides a comprehensive view into the threat landscape across client base
- Helps to quickly identify threats to enable quick resolution
- Robust reporting helps value realization



Thank You!

Chris Wruck

Computer Guts, LLC

cwruck@computerguts.net

715.333.3456

www.computerguts.net