

BENCHMARKING YOUR IT SECURITY FOR BUSINESS SUCCESS

Preparing for budget season? It's time to prioritize your security roadmap and benchmark your business' IT security to know where you should invest. But IT security is so broad and complex it can be overwhelming to know where to start and what to prioritize. That's where ZAG's 25 years of IT experience can benefit your business.

ZAG'S 10 IT SECURITY BEST PRACTICES

Benchmark your current security posture and see what steps you need to take to ensure your infrastructure is strong enough to defend against ever-evolving sophisticated cyberattacks.

1

MODERN ANTIVIRUS

Today's threats are customized, and your old one-size-fits-all antivirus won't prevent hackers from breaching your network. Modern antivirus solutions stop signature-based and crypto attacks from successfully executing across your network.

2

SERVER & DESKTOP PATCHING

You operate 24/7/365 and uptime is not negotiable. So too is ensuring your security is up to date, meaning patching is critical. As with any of your equipment, your technology needs to be regularly maintained with consistent, predictable system updates and patching.

3

MODERN DNS PROTECTION

This is your first line of defense, stopping employees from accidentally visiting malicious website from which criminals launch cyberattacks. Secure DNS services (like Cisco Umbrella) protect your users and their devices—on and off your network.

4

DMARC: DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING & CONFORMANCE

Cybercriminals send fake (spoofed) emails posing as company executives to coerce sensitive information and cash from unaware users, often in the Finance department. This is known as spear phishing. DMARC is an email authentication protocol that helps prevent these kinds of attacks.

5

MODERN ANTISPAM

Cyberattacks via email are continuously happening—a flood of spam and phishing attacks—trying to breach your network or access your bank accounts. Don't rely on the systems that come as part of your default service. Invest in a modern antispam solution that actively keeps the criminals out.

Only 73% of companies have modern antispam protection in place*

6

DISASTER RECOVERY PLANS

Having a written and tested Disaster Recovery Plan in place today can help your team know what to do when a disaster strikes tomorrow—whether natural, operational, or cybersecurity-related. This reduces the potential damage and quickly restores operations when one occurs.

Only 44% of companies have a written Disaster Recovery Plan*



MULTIFACTOR AUTHENTICATION (MFA) IS 3-FOLD

Email and Business Applications

Remote Access

Servers

7

MFA FOR OFFICE 365, EMAIL & BUSINESS APPLICATIONS

Criminals are great at getting people to give up their email account passwords, especially executives. Multifactor Authentication services (like Cisco Duo) significantly decreases the chances that cybercriminals can access your network, even if they were able to steal user login information.

8

MFA REMOTE ACCESS

With remote and hybrid work models, everyone should be using MFA for remote access. It's easy for employees to access what they need to do their jobs and hinders cybercriminals from breaking into your network. From financial information to sensitive corporate and personal identifiable data, MFA protects it.

Only 76% of companies have remote MFA

9

MFA ON SERVERS

Your most critical corporate resources are stored on servers, and just like email and remote access, securing these assets is essential. Enabling MFA on servers is another line of defense against compromised IT admin credentials, whether from email phishing or stolen passwords.

Only 48% of companies have MFA on servers

10

INCIDENT RESPONSE PLANNING

IT incidents are inevitable. From data center failures to the increased risk of cyberattacks. An IR Plan is a playbook for how your organization responds to and resolves information security and major information technology incidents.

Only 32% of companies have an Incident Response Plan in place

BENCHMARK YOUR SECURITY POSTURE WITH ZAG

If you are missing any of these vital components for a strong security posture, it's time to catch up before cybercriminals catch you. ZAG can help you close these gaps.



STRENGTHEN YOUR SECURITY WITH ZAG

Schedule your free external security posture review today, so you know how to invest for tomorrow. Want to learn more about how Incident Response Planning can benefit your business? Contact us and we'll tell you all about it.

[Get Started](#)

* All stats are from a private Manufacturing/F&B/Ag industry survey report.