ALTOURAGE

CYBERSECURITY PRIMER

THE COSTS OF
DATA THEFT, EXPOSURE & LOSS

RISK OR THREATS TO YOUR CUSTOMERS' (CONFIDENTIAL/PRIVATE) INFORMATION AND DATA

DOWNTIME DISRUPTION AND LOST PRODUCTIVITY

COMPETITIVE ADVANTAGE OR CORPORATE ESPIONAGE

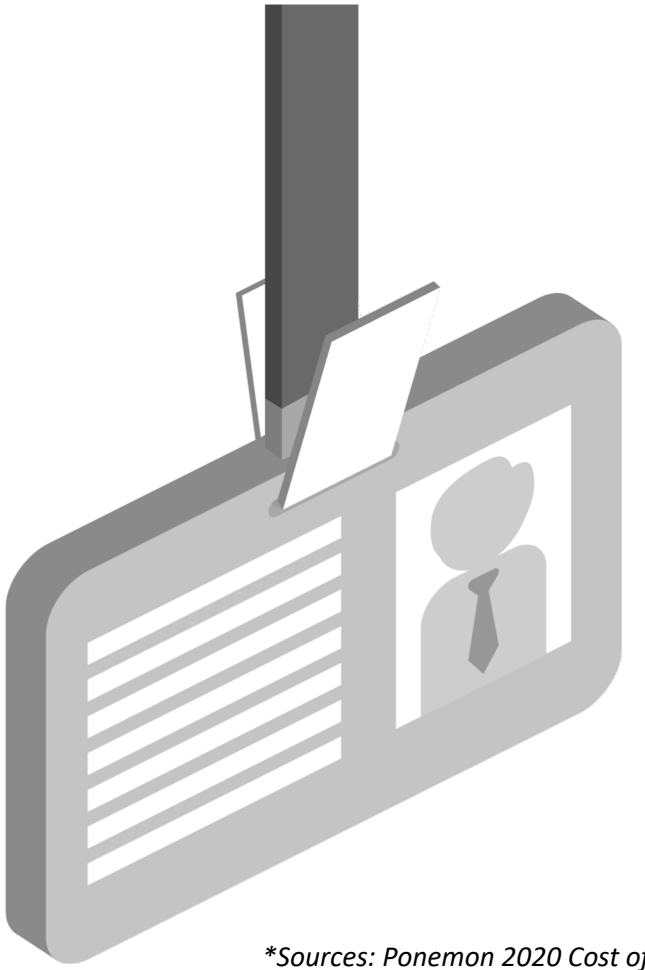
LOSS OF CUSTOMERS AND FUTURE BUSINESS

EXPOSURE TO LEGAL ACTION OR REGULATORY PENALTIES

BRAND OR REPUTATION DAMAGE

Common Cybersecurity Threats

Insider Threats

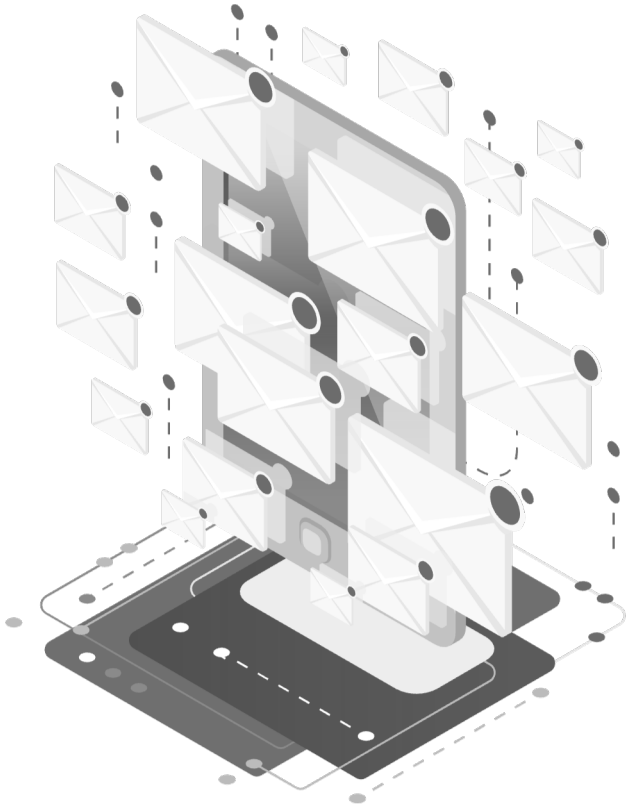


63% of insider-related cybersecurity incidents can be traced back to negligent or careless users.

**Sources: Ponemon 2020 Cost of Insider Threats Global Report & Bitglass 2020*

ALTOURAGE

Business Email Compromises



"Over a third of respondents (36%) were not confident that employees at their organizations would be able to spot and avoid an email phishing attack in real time."

Source: Phishing Attack Landscape Report 2020

ALTOURAGE

Phishing

Beware of phishing attacks that attempt to obtain sensitive information, such as usernames, passwords, or credit credentials, under the guise of a trustworthy entity.

ALTOURAGE

Spear-Phishing

Phishing has evolved into “Spear-Phishing” a more targeted version of traditional phishing, through which hackers spend time getting to know you via social media.

ALTOURAGE

Ransomware

Ransomware is a type of malware that locks your computer screen and prevents you from accessing your computer or data until you pay a ransom.

While ransomware has long been one of the main cyberthreats to businesses, the past 6 to 18 months have seen organizations more exposed than ever before.

ALTOURAGE

Cybersecurity Best Practices

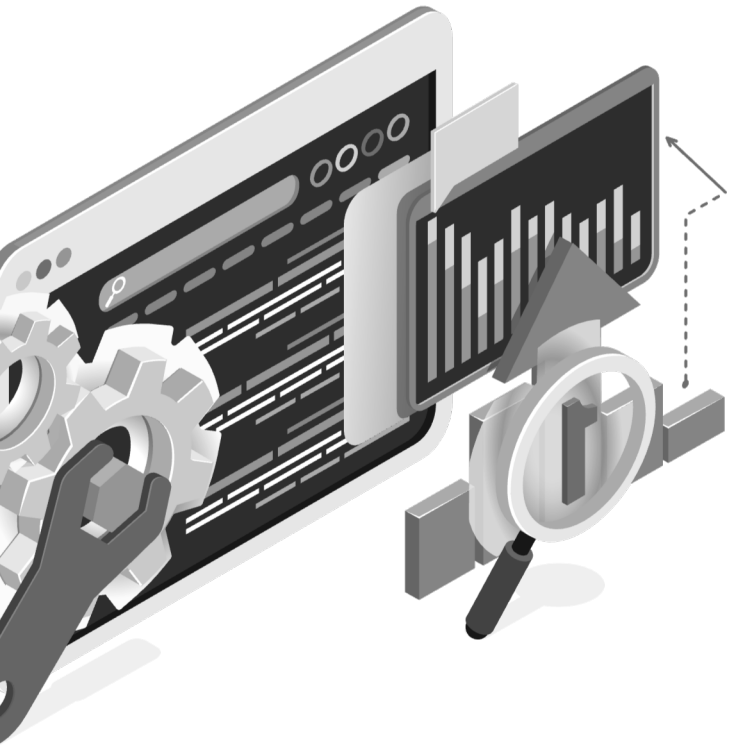
Patch Management

Automate System Updates

Patching is the process of repairing system vulnerabilities discovered after the infrastructure components have been released in the market. Patches apply to many different systems including operating systems, servers, routers, desktops, email clients, mobile devices, firewalls, etc.

ALTOURAGE

Access & Permission Controls



Implement the Principle of Least Privilege

Only the right users have access to the necessary systems, applications and data. Admin or full permission privileges are restricted to only those expressly necessary for staff, employees and third-party vendors or suppliers.

ALTOURAGE

Identity Authentication & Password Security

Most passwords today are too guessable or are being sniffed or captured by hardware from software keyloggers.

2FA or MFA are a combination of individual security factors required simultaneously to prove a user's authentic identity.

ALTOURAGE

Advanced Email Security

- Email is often the gateway to your network.
- Effective anti-spam software is essential to keeping malware at bay.
- Most email providers include anti-spam software, but it needs to be carefully tuned to be effective.
- On-premises email servers and some hosted environments need third-party software (and updates).

ALTOURAGE

Regular Security Risk Assessments

- Don’t just assume that your firewall, anti-virus, and anti-malware solutions are doing the job. Be certain.
- Security is not a one-and-done effort.
- The security landscape changes daily.
- Vulnerability scans should be run at least monthly to confirm the security of your network.

ALTOURAGE

Security Awareness Training for Employees

The #1 Security Risk is “the unit between the desk and the chair.” Regular education and constant vigilance will do more for your security than all the security software in the world.

ALTOURAGE