About Michael Argast

- 20+ years in Information Security

- Career spans operations, security sales, leadership, consulting

- Roles at Sophos, TELUS, Kobalt.io

- Well connected to local and international community - member of Vancouver ISACA, Provincial Security Advisory Committee, SecSig and more

- Presented/press internationally - Moscow InfoSec, Oxford University, New York Times, Associated Press.

- Father of three girls, into camping, snowboarding, travel

KOBALT.IO

Cybersecurity is an investment in your business

Protecting sensitive data

Safeguard this information from theft or unauthorized access, protecting both the business and its customers

Maintaining trust

Data breaches and cyber attacks can significantly damage a business's reputation and erode customer trust

Compliance

Many industries have regulatory requirements for cybersecurity, and non-compliance can result in hefty fines or legal penalties

Cost savings

A cyber attack can be incredibly costly for a business, resulting in lost revenue, legal fees, and damage to the brand's reputation

KOBALT.IO

KOBALT.IO

Understanding Cybersecurity

Monitoring
House alarm system for inside and outside threats
Managed Security Operation Center · Alarm Company

Incident Response Plan · Fire plan
Tabletop · Fire drill

Compliance & Privacy
Building codes and inspections

Access Control
Who should have which keys

Firewall · Fence
Anti-virus · Guard

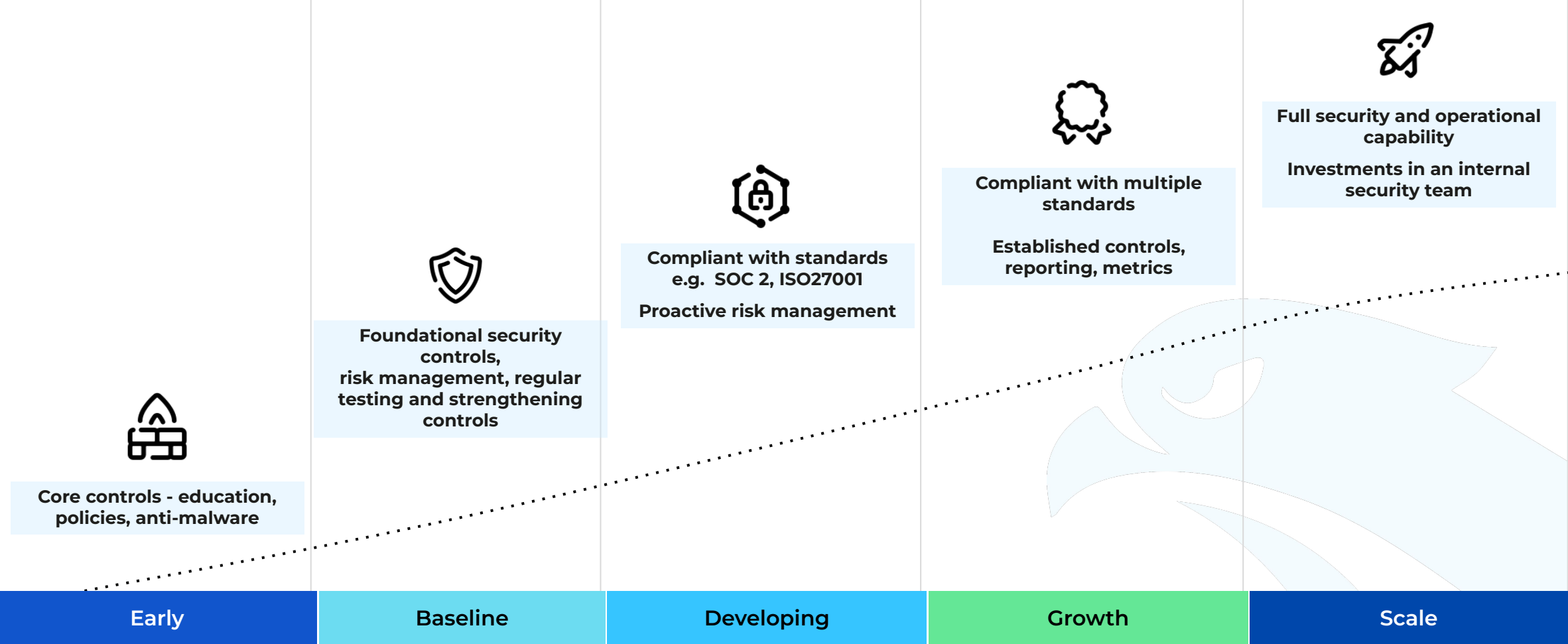**Gap Assessment**
Visiting a doctor for a checkup

Vulnerability Management
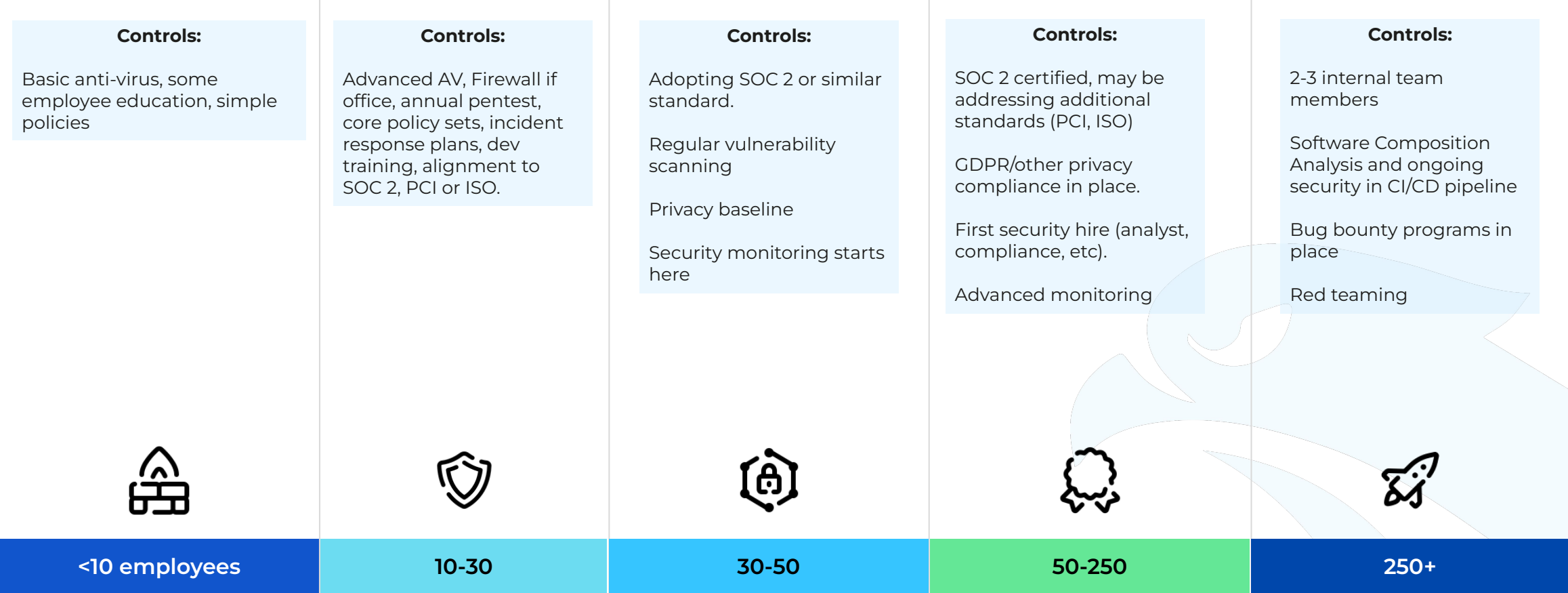Is your building using up-to-date materials that are resistant and conform to codes?

Penetration Test
Checks if the front door or windows are properly locked, and if not, see how far inside one can go
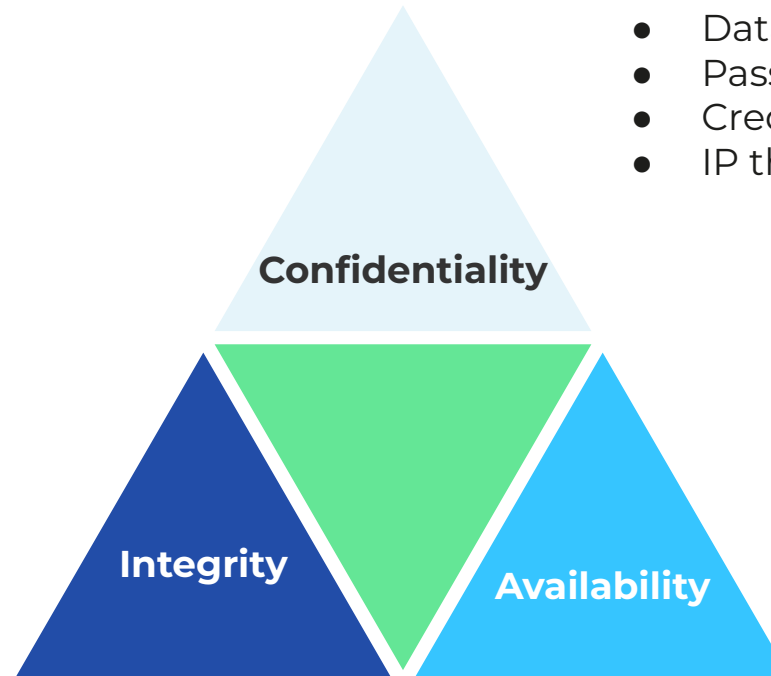
User Education
Watching news and picking up new and better ways to protect your home

Cybersecurity Adoption

Full security and operational capability

Investments in an internal security team

Compliant with multiple standards

Established controls, reporting, metrics

Compliant with standards e.g. SOC 2, ISO27001

Proactive risk management

Foundational security controls,
risk management, regular testing and strengthening controls

Core controls - education, policies, anti-malware

| Early | Baseline | Developing | Growth | Scale |

KOBALT.IO

Risk Level

Typical Size And Control Adoption

Controls:

Basic anti-virus, some employee education, simple policies

Controls:

Advanced AV, Firewall if office, annual pentest, core policy sets, incident response plans, dev training, alignment to SOC 2, PCI or ISO.

Controls:

Adopting SOC 2 or similar standard.

Regular vulnerability scanning

Privacy baseline

Security monitoring starts here

Controls:

SOC 2 certified, may be addressing additional standards (PCI, ISO)

GDPR/other privacy compliance in place.

First security hire (analyst, compliance, etc).

Advanced monitoring

Controls:

2-3 internal team members

Software Composition Analysis and ongoing security in CI/CD pipeline

Bug bounty programs in place

Red teaming

| <10 employees | 10-30 | 30-50 | 50-250 | 250+ |

← Fintech/Healthtech typically achieves security one size earlier

Risk Level

The CIA Triad - Risk Management

Attacks on confidentiality:
- Data breaches
- Password dumps
- Credit card theft
- IP theft

Confidentiality

Attacks on integrity:
- Email/wire transfer fraud
- Impersonation attacks

Integrity

Availability

Attacks on availability:
- Denial of service attacks
- Ransomware attacks

KOBALT.IO
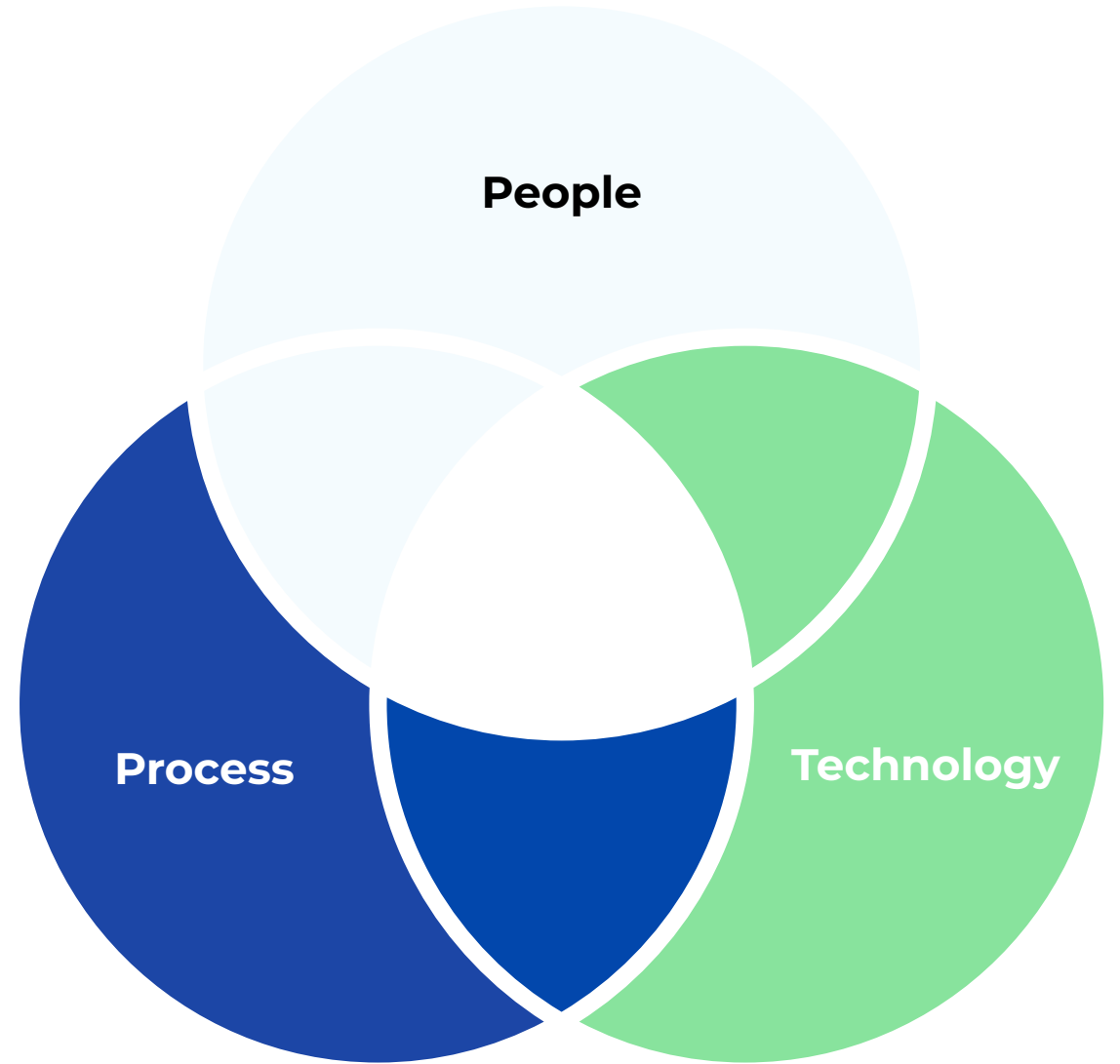
Remote Work Cybersecurity

Secure Network

Endpoint Protection

Security Awareness Training

Strong Password and MFA

KOBALT.IO

What is Endpoint Protection

Endpoint Security

- Malware Prevention
- Internal Threats
- Access Levels

- Device Control
- Data Loss Prevention
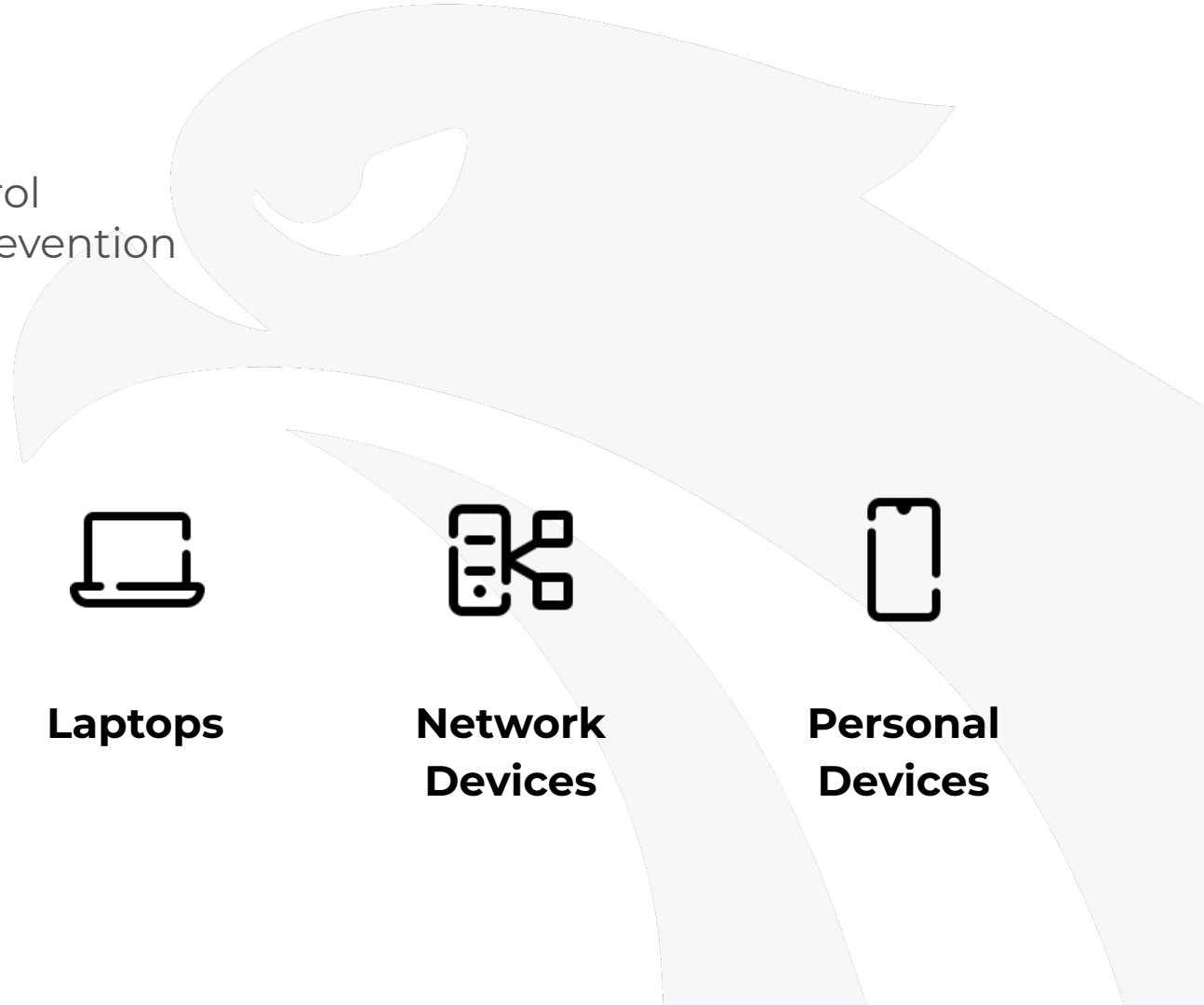
Server   **Desktops**   **IOT Devices**   **Laptops**   **Network Devices**   **Personal Devices**

KOBALT.IO

Why You Need Strong Endpoint Security If All Your Data Is In The Cloud?

- **User Devices as Entry Points**: All cloud data is accessed through user devices, making them critical targets
- **Account Compromise Risk**: Attackers can steal passwords, authentication tokens, and data directly from logged-in applications
- **Developer Laptops Vulnerability**: Malicious code/backdoors can be injected via compromised developer laptops, bypassing application security measures
- **Sophisticated Attacks**: Modern threats can compromise even experienced users through methods like drive-by downloads and remote exploits
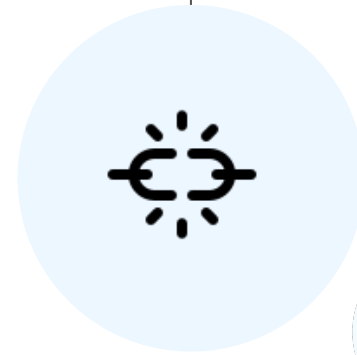
How Business Email Compromise Works

💡 Tons of sensitive data is held inside email accounts

Escalate Privileges

Lateral Movement: Pivot to other accounts

Identify a victim

Account Compromise

Leverage for more sophisticated attack

Coercive control

Maintain Presence: Attackers stay quiet, look for more loopholes

Impact increases over time

▶ ▶ ▶   ▶ ▶ ▶

PREVENTION   **RESPONSE**

KOBALT.IO

Preventing Business Email Fraud
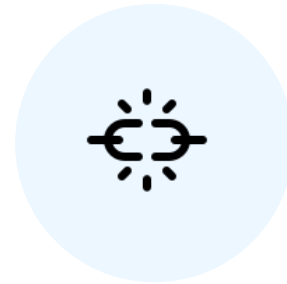
User Education
➜ prevent phishes, credential stuffing

Endpoint Protection
➜ Detect ransomware, data theft, breaches and more

Vulnerability Scanning
➜ help ensure strong external posture

Email Security Standards
➜ detect and prevent lateral movement

Managed Threat Detection
➜ detect account compromise, preventing long term dwell times

Email Spoof Prevention and Domain Detection
➜ reduce risk of impersonation attacks

Fraud Prevention Training
➜ teach financial staff how to prevent transfer fraud

NO PROFIT!

KOBALT.IO

KOBALT.IO

Cybersecurity Awareness Kit

Get ready to boost your security game with this kit!

Cybersecurity Awareness Kit

Here's what you will get:

- A 1-min video that helps you understand basic cybersecurity
- A 2-minute video that explains Business Email Fraud
- Refreshed Business Email Fraud Webinar*
- Top 3 cybersecurity solutions every business should have*
- Refreshed Training Calendar*
- A free Ransomware Incident Response Playbook

Download Now

https://landing.kobalt.io/cybersecurity-awareness-month-kit-download

KOBALT.IO

✉ info@kobalt.io   in /kobaltio

🌐 https://kobalt.io   𝕏 @kobaltio

Book a meeting