Kalles/Group

CYBER RISK / SECURITY BASICS

Threat landscape

ORGANIZATIONS OF ALL SIZES AND TYPES ARE INCREASINGLY EMERGING AS PRIORITY TARGETS OF THESE ATTACK METHODS.

Social Engineering: The use of deception to manipulate individuals into divulging confidential or personal information.

Malware: Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Phishing: Emails that appear to be from a reputable company or person attempting to collect personal information.

Ransomware: A type of attack where malware blocks access or threats to expose information until a ransom is paid.

Spear Phishing: Sending emails pretending to be a familiar sender attempting to reveal confidential information to targeted individuals.

Ability to counter quickly when new protective measures are introduced.

Challenges

ORGANIZATIONS ENCOUNTER THESE COMMON CHALLENGES WHEN LOOKING TO MAKE MEANINGFUL INVESTMENTS IN CYBERSECURITY CAPABILITIES

Financial

SPEND SCRUTINIZED AT A MICRO LEVEL

Every dollar matters. Minimal tolerance for expenditures not directly and visibility tied to financial value.

Fragmentation

FUNCTIONS RESOURCED ACROSS A CONDENSED TEAM

Staff are perpetually busy and requires to be highly functional re task switching and responding to sometimes unpredictable demands.

Expertise

ALIGNED WITH THE ORGANIZATION'S CORE COMPETENCIES

Team is built to deliver the expertise and proficiency needed to drive for mission success. Taxing to cultivate secondary and peripheral expertise.

Tools

ALIGNED WITH REVENUE AND MARGIN DRIVERS

Technologies and solutions connected to driving for consistent and predictable financial results. Difficult to invest in supplemental tooling even when value to clear.

Prioritization

ALIGNED PRIMARILY WITH NEAR-TERM TARGETS

Top-line priorities are self-evident and demand significant portion of budget and resource investment. Perpetually managing a backlog of next set of priorities.

CYBER RISK / SECURITY BASICS

Checklist Baseline Practices

ORGANIZATIONS SHOULD BE INTENTIONAL ABOUT THE CAPABILITIES THEY HAVE IN EACH OF THESE AREAS

HIGH PRIORITY

PRACTICE	CHECKLIST ITEMS
User Training (continuous)	○ Phishing Awareness ○ Secure User Habits (do's and don'ts) ○ Awareness of Regulatory Requirements ○ Remote Working
Technology Hardening	○ Mobile Devices ○ Network Assets ○ User Assets ○ Remote Working ○ Storage ○ Cloud
Endpoint Management	○ Laptops ○ Servers Virtual Machines Cloud-based Endpoints

PRACTICE	CHECKLIST ITEMS
Vulnerability Management	○ Laptops ○ Servers ○ Virtual Machines ○ Cloud-based Endpoints ○ Network Assets
Data Handling & Protection	○ Encryption ○ Secure Email ○ Secure Document Handling ○ Data Classification ○ Data Handling Procedures

MEDIUM PRIORITY

Resilience & Reliability	○ Business Continuity Planning ○ Disaster Recovery Planning ○ Technology Redundancy/Failover/Recovery
Security Operations	○ Detection and Response – Events ○ Detection and Response – Anomalies ○ Detection and Response - Etc.

Third-Party Risk Management	○ Due Diligence
Incident Response	○ Process Definition ○ Process Testing (tabletop) ○ Process Refinement ○ Process Training