“In cyberspace, there exists no safe harbor. Every organization with a digital presence is exposed like an island amidst an angry, implacable ocean that seems to send wave after wave of cyberattack.”

—Matt Miller, BeyondTrust

**COMMON TRIP HAZARDS**

- **Phishing Attacks**: Masquerading as trusted entities to deliver malicious links via email.
- **Ransomware**: Encryption of victim’s data which is held until a set ransom is paid.
- **Zero-Day Exploits**: Exploitation of vulnerabilities that don’t yet have an available patch.
- **Man in the Middle (MiTM)**: When a hacker intercepts and decrypts a victim’s communication.
- **Insider Threats**: A threat that comes from within an organization (employees, contractors).
- **DDoS Attacks**: Distributed denial of services by overwhelming target with traffic.

**TIP #1**: Protect Your Privileged Identities

**TIP #2**: Secure Remote Access

**TIP #3**: Apply Endpoint Privilege Management

**TIP #4**: Apply Hardening & Vulnerability Management

**TIP #5**: Prevent Tampering of Mobile & Remote Endpoints

**TIP #6**: Secure & Empower the Service Desk

**TIP #7**: Perform Remote-Worker Penetration Testing

**RECALIBRATE YOUR SECURITY FOR TODAY’S CYBER THREATS**

94% of companies experienced a business-impacting cyber-attack or compromise over the last year.

791,790 Record-breaking number of cybercrime complaints received by the FBI in 2020.

630% Increase in early 2020 of threat activities waged on cloud services by external actors.

Get Your 2022 Cybersecurity Survival Guide