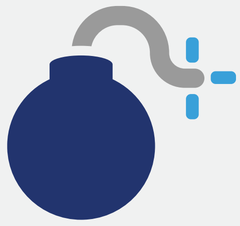
The Top Five Security Threats to Your Business

Cyber security breaches are more common now than they have ever been. While they don't all make news headlines, they affect numerous businesses every single day.

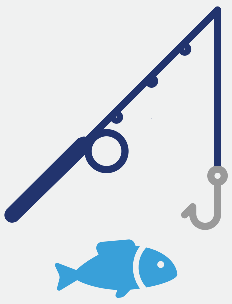
What exactly are these threats? How are they carried out and how can they impact business? The Level 3℠ Advanced Threat Intelligence team has identified the top five most common security threats that you should know about.



1 Network and Application Layer Attacks

- Disruption or suspension of servers and network resources connected to the Internet.
- Easy attack for anyone to launch, very difficult for businesses to resolve on their own.
- DDoS attack packages available to anyone on the black market for very little money.

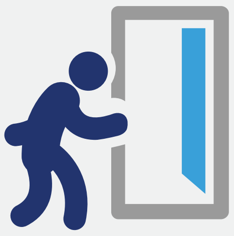
Also Called: Denial of Service (DoS) or Distributed Denial of Service (DDoS)
Frequency: Very common



2 Social Engineering

- Fake email or other electronic communications used to acquire access or information.
- Difficult to detect, often the source appears legitimate.
- Critical information about your enterprise falls into the wrong hands.

Also Called: Phishing or Spear Phishing
Frequency: Common and ongoing



3 Advanced Persistent Threats

- "Backdoor" to your systems is established using vulnerabilities.
- Gather administrative credentials and exfiltrate data.
- Attackers use custom malicious code, remain undetected for as long as possible to continue to do damage.

Also Called: APT
Frequency: Increasing every year

4 Organized Cybercrime

- Risk of intellectual property theft, confiscated bank accounts, and loss of customers as a result of business disruption.
- Ultimately easier to prevent than to fix, cyber criminals specialize in selling personal information on the black market, using ransoms and blackmail.

Also Called: Cybercrime Syndicates
Frequency: On the rise

5 Major Data Breaches

- Through a variety of methods, sensitive information about enterprise companies in every industry is exposed.
- Business is disrupted, customer and company data is compromised, and recovery costs are enormous.
- Financial, media and entertainment, health care, retail and many more are vulnerable.

Also Called: Hacked, Accidentally Published, Poor Security, Lost/Stolen Media, Inside Job
Frequency: In the news every month

Level 3 Helps Secure and Protect Your Bottom Line

The risks identified by Level 3's Security Operations Center are all serious. Whether it's the loss of critical information about your company or your employees, no company can afford the financial impact. And the problems don't stop there: Damage to your reputation and harm to customer confidence can be devastating.

Level 3's network-based solutions use a defense-in-depth approach. We pair network defense strategies with Unified Threat Management (UTM) services for monitoring traffic irregularities, and network firewalls. Let Level 3 help you secure your most sensitive, private data. Talk to your Level 3 representative to learn why the Security Solutions services are everything you need to have your bases covered.

Let's Connect

Please don't hesitate to contact your Level 3 sales representative with questions about network security and protecting yourself against major threats.

Level(3)® COMMUNICATIONS

Connecting and Protecting
the Networked World℠