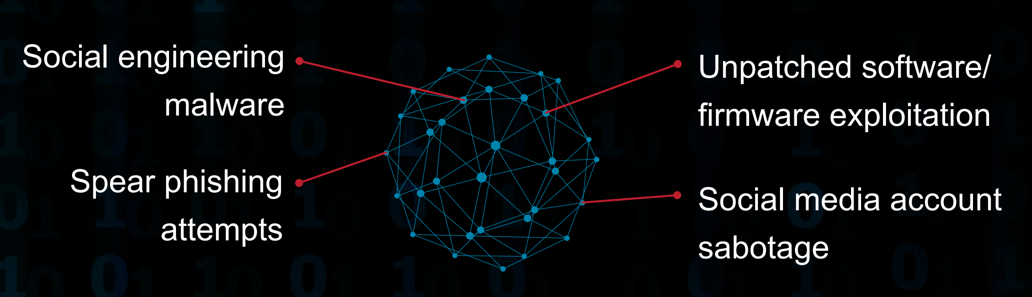
TOFFLER
ASSOCIATES

CYBER RISK TO YOUR ORGANIZATION’S FUTURE VALUE

Cloud computing, artificial intelligence, mixed reality (augmented and virtual reality), blockchain, and even cryptocurrencies are emerging as pillars of any enterprise transformation. This has resulted in hyper-automated processes, accelerated supply chain productivity, and growing customer loyalty. But, as organizations digitally transform to create and enhance their future value for their workforce, customers, and shareholders, they are exposing themselves to more cyber risk.

Organizations must anticipate future threats and take control of the risky environment. To start, organizations must understand the evolution of technology and cyber threats – **past, present, and future** – as they test new business models and adopt new technology.

PAST THREATS

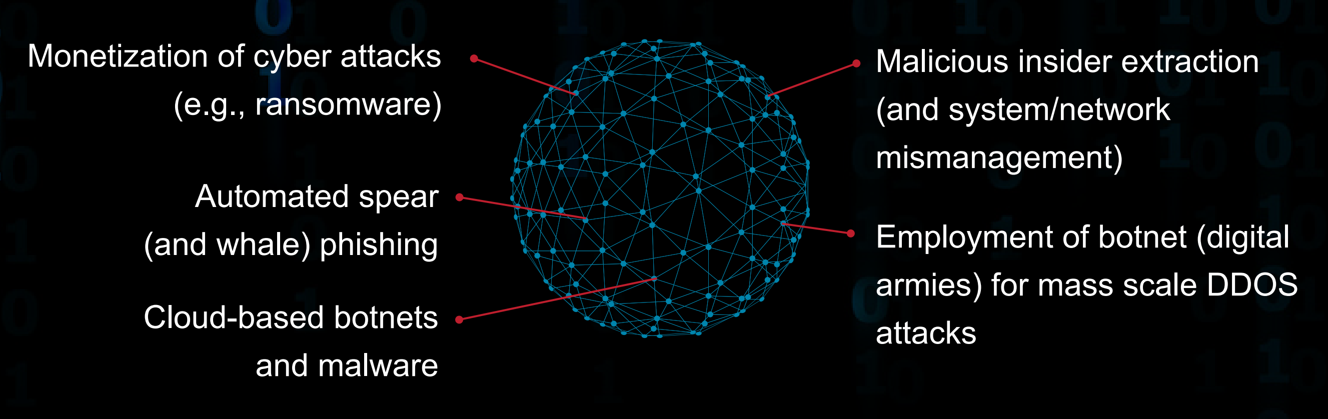

Social engineering malware
Spear phishing attempts
Unpatched software/ firmware exploitation
Social media account sabotage

The Aftermath:

- Stolen credit card numbers
- Exfiltrated SSNs
- Names, addresses, and other PII dumped online (doxing)

Past Threat Example:
The Associated Press news agency’s Twitter account was hacked. The hackers created a fake tweet stating two explosions occurred at the White House and that President Obama was wounded.

PRESENT THREATS

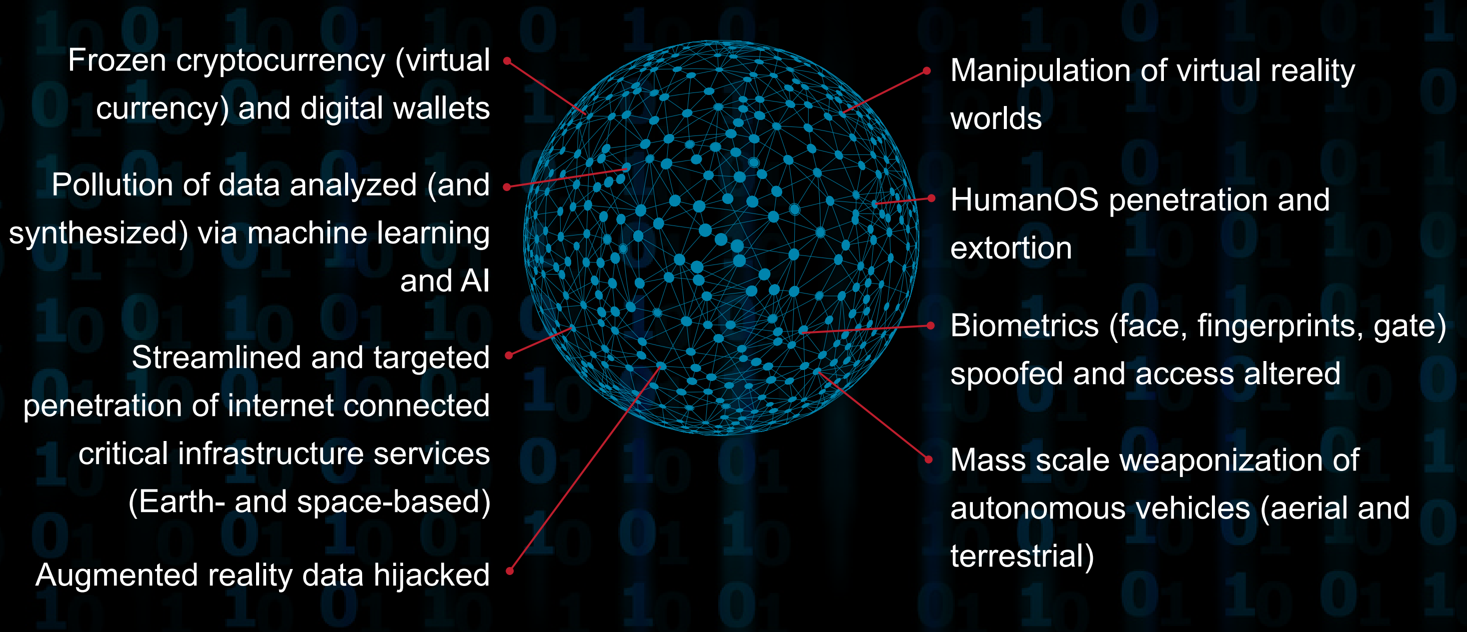

Monetization of cyber attacks (e.g., ransomware)
Automated spear (and whale) phishing
Cloud-based botnets and malware
Malicious insider extraction (and system/network mismanagement)
Employment of botnet (digital armies) for mass scale DDOS attacks

The Aftermath:

- Volumes of personal health, financial, and other records exfiltrated
- Covert information operations conducted to influence perception of a market segment
- Unauthorized access (and black market/dark web resale) of millions of corporate and government records

Present Threat Example:
After penetrating an India-based payment processor of prepaid Visa and MasterCard credit cards, hackers were able to withdraw $5 Million from 4,500 bank accounts. Two months later, an additional $40 million was stolen from bank accounts using 36,000 transactions.

FUTURE THREATS


Frozen cryptocurrency (virtual currency) and digital wallets
Pollution of data analyzed (and synthesized) via machine learning and AI
Streamlined and targeted penetration of internet connected critical infrastructure services (Earth- and space-based)
Augmented reality data hijacked
Manipulation of virtual reality worlds
HumanOS penetration and extortion
Biometrics (face, fingerprints, gate) spoofed and access altered
Mass scale weaponization of autonomous vehicles (aerial and terrestrial)

The Aftermath:

- Targeted and immediate financial devastation across markets
- Hyper-arbitrage of critical information
- Theft of intellectual data (altering decisions for the worst)

Future Threat Example:
Multi-million dollar smart contracts eliminated overnight. This would freeze digital assets and dry up commerce across multiple consumer and supplier segments - causing billions in damage (reputation, financial, environmental, and regulatory)

What does this mean?

Given where the future cyber threats are going, leaders are faced with a tough decision – “should I invest in the security of my products and platform (risk) at the cost of innovation and open collaboration (reward)?”

Too often, this spectrum – *all in* on security or *all in* on innovation – has become an “either or” decision point. Leaders seek higher ROIs and underinvest in risk management processes, because they do not fully understand the value of investing in risk management. This has led to more cyber incidents and breaches that have caused business, reputation, and regulatory concerns.

What must leaders do to embrace risk for the sake of agility, being first (or fast) to market, and not experience the chaos in the aftermath of a cyber-attack?

What should leaders do?

Exercise organizational “self-awareness”

Know what your business model is. Know what value (tangible and intangible) you provide for your workforce and consumer. Understand what your assets are (obviously data, but what specific kind?). Take those into consideration and review your cyber risk appetite. The tug between business and security investments will always be a dilemma for leaders. Understand the magnitude of your cyber risk profile and its impact on your business outcomes. Build and iterate different investment scenarios that incorporate low, medium, and high levels of risk impact. Prioritize what generates value for your workforce and consumer segments. Be honest with yourself: AVOID the “this won’t happen to us” attitude.

Demassify cybersecurity

Yes, it’s different from what’s been the status quo, but crime-as-a service, cyber espionage, and cyber gangs are constantly innovating. At the same time, trust in institutions is deteriorating, thanks to the barrage of recent cyber incidents and breaches. It’s time you apply a different mental and business model to your security strategy, so you can empower your business lines and units with the proper foresight, knowledge, training, and tools to detect and remediate any vulnerabilities while sharing threat intelligence. Talk to your customers and third-party suppliers. Understand what their future concerns are and rebuild their trust.

Test, test, and test

...your cyber risk readiness and resilience over and over again. Demassify your audience who you test with. Invite outside parties and design scenarios focused on future vulnerabilities and threats. Using those scenarios, administer methods, such as war gaming, table top exercises, or penetration testing to find holes within existing strategy, resiliency plans, and operational processes and procedures with the intention of remediating it.

Is your organization prepared for today’s and tomorrow’s cyber risk?

Contact us to start a conversation!

About Toffler Associates

Toffler Associates is a strategic advisory firm that helps businesses and public entities capitalize on opportunities, build agility, and mitigate risk in an uncertain future. Our unwavering commitment to being a catalyst for change is backed by a Future Proof® business consulting approach. We help global leaders ask the right questions, understand how future shifts impact current decisions, and position their organization to create future value.

TOFFLER
ASSOCIATES

linkedin.com/company/toffler-associates
www.TofflerAssociates.com
@TofflerInsights