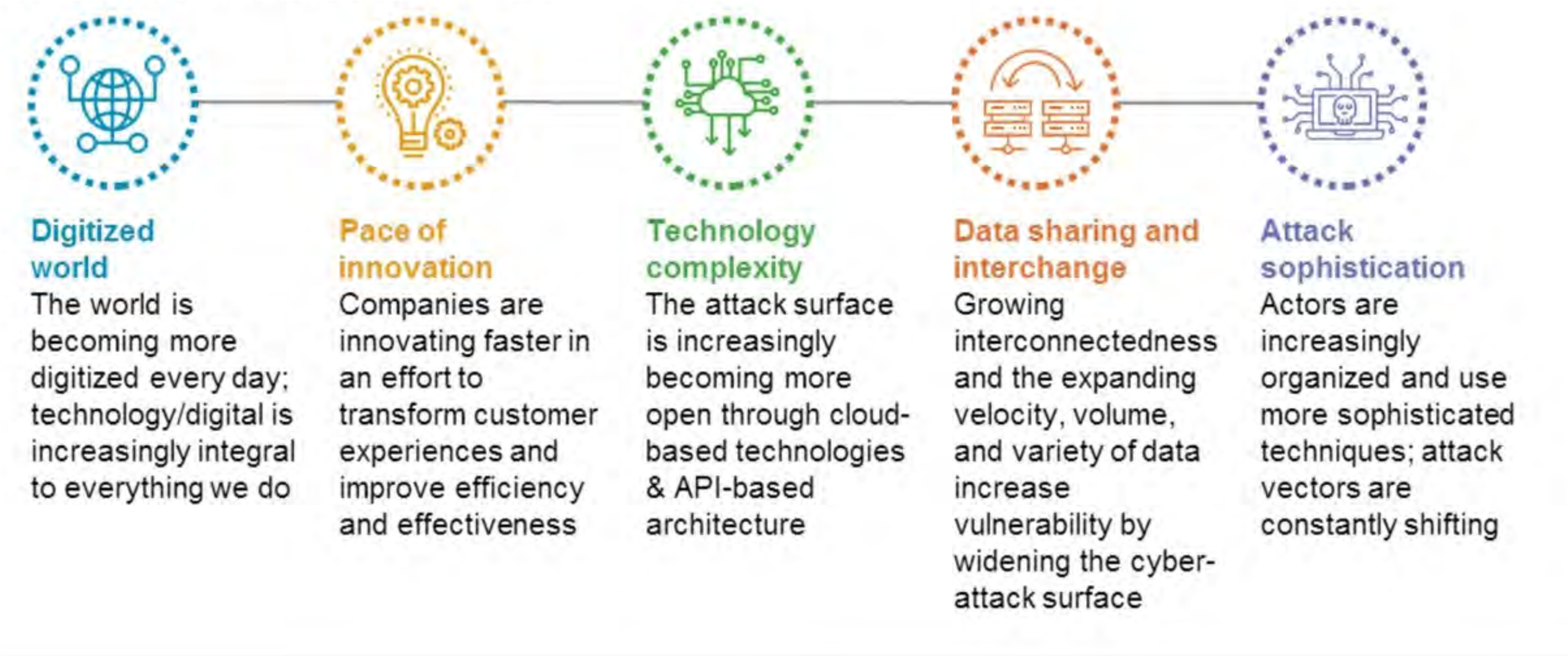
Implementing a Culture of Cybersecurity

Clear and Present Danger

- Cyber attacks and security breaches are **increasing** in frequency and sophistication, with discovery after the fact, **if at all.**
- Targeting of organizations and individuals with malware and anonymization techniques that can **evade controls**.
- Current perimeter-intrusion detection, signature-based malware, and anti-virus solutions are providing **little defense** and are rapidly becoming obsolete— Criminals use encryption technology to avoid detection.
- Criminals are **leveraging innovation** and moving at a pace security vendors cannot possibly match.

Drivers of Increased Cyber Risk



Digitized world
The world is becoming more digitized every day; technology/digital is increasingly integral to everything we do

Pace of innovation
Companies are innovating faster in an effort to transform customer experiences and improve efficiency and effectiveness

Technology complexity
The attack surface is increasingly becoming more open through cloud-based technologies & API-based architecture

Data sharing and interchange
Growing interconnectedness and the expanding velocity, volume, and variety of data increase vulnerability by widening the cyber-attack surface

Attack sophistication
Actors are increasingly organized and use more sophisticated techniques; attack vectors are constantly shifting

Our Cyber Reality

“206 days is the average mean time to identify (MTTI) a breach” — *Ponemon, 2019 Report*

“73 days is the average mean time to contain (MTTC) a breach” — *Ponemon, 2019 Report*

“SMBs are out of business within six months of discovering they had a data breach, *U.S. Congress*

31% of data breach victims later experience identity theft — *Experian*

Physical breach is not necessary to undermine confidence, question integrity or minimize access

Attackers use automation to move fast and deploy new threats at breakneck speeds

Open source projects are turning into malware distribution channels - Up 430% in the last year - *Sonatype*

Cybersecurity Maturity Model

- The Department of Defense (DoD) announced the Cybersecurity Maturity Model Certification (CMMC) on January 31, 2020. The regulatory framework is a unified standard that stipulates the cybersecurity requirements that must be implemented across the entire Defense Industrial Base (DIB).

Internet of Things (IoT) Cybersecurity Improvement Act of 2020

- According to the IDC, there will be at least 55.7 billion connected devices by 2025, with IoT accounting for 75% of all devices. The IoT Cybersecurity Improvement Act of 2020, enacted on December 4, 2020,to establish the minimum current cybersecurity standards to be included in IoT devices used by the Federal Government. As such, the law currently applies to federal government agencies only.

General Data Protection Regulation

- The EU’s GDPR is one of the global regulations that protect the sensitive personal information of EU citizens. The regulation is mandatory for all organizations that collect user data belonging to citizens of EU countries.

State Data Privacy Rules

- Different states have implemented variating data privacy regulations. At least 38 states have considered or introduced not less than 280 new regulations that significantly focus on cybersecurity compliance. For example, the California Consumer Privacy Act (CCPA), which was enforced in January 2020.

National Defense Authorization Act

- There were roughly 37 cybersecurity amendments in this fiscal year’s NDAA, many of which will have a positive and increased impact within the ICS/OT space. The NDAA for FY22 addresses a handful of cybersecurity topics and trends respectively addressing roles of the DoD and CISA to implement more robust cybersecurity programs and practices.

Chasing the Security Culture

- The old saying is “knowledge is power.” We disagree.
- What you do with the knowledge is the consequential value of having the knowledge.
- Security is the art of engineering solutions based on the available information we derive from research, experience, inference, requirements and threat intelligence.
- This knowledge allows us to build an integrated system and a to build a culture that continuously seeks **visibility of assets**, **understanding of interdependencies** and **each person’s role.**

QUESTIONS

Michael Echols

CEO, Max Cybersecurity

mechols@maxcybersecurity.com

Connect on LinkedIn

https://linkedin.com/in/Mechols

https://maxcybersecurity.com