Only a Culture of Cybersecurity will Save US

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

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.

The weakest link in cybersecurity is now people, not devices. As such, the human factor is considered the biggest threat to cyber security.

Cost of Financial Breach

According to the Ponemon Institute's Cost of a Data Breach Report, an annual compendium of data breach trends that over the years has become a barometer of sorts for the information security industry, in 2020, data breaches on average cost $3.86 million.

- Financial services attacks are some of the costliest, with an average cost of $18.3 million per breach.
- 90% of attacks start with a highly targeted spear-phishing email that gives hackers access to a company's servers.
- Hackers gained access to, on average, 352,771 files per financial services breach.

THREATS TO US ECONOMY

Cyberattacks on major financial institutions pose one of the biggest threats to the US economy, with the potential to cripple the system

Federal Reserve Chairman Jerome Powell has warned that the biggest risk to the US economy is the threat of cyberattacks, which could bring financial institutions to a halt by taking away their ability to track payments.

Federal Reserve is keeping its "eyes on the most now is [the] cyber risk," laying out a situation in which a hack could easily take financial institutions offline.

BY WHOM

Chinese are exploiting the US and other Western networks and systems to get an advantage in the cyber domain.

Russia has utilized its cyber capabilities to influence elections in the U.S. and Europe. In addition to election meddling, Moscow is heavy into espionage.

North Korea primarily utilizes the cyber domain for financial gains and to evade UN sanctions. Essentially, Pyongyang acts as an organized crime group.

Iran employs its cyberwarfare capabilities against the US but also for influence operations in the Middle East and Europe.

U.S. Cyber Command Commander, National Security Agency Director and Central Security Service Chief Gen. Paul Nakasone

Democracy is under threat!

- Elections
- Evidence - Chain of custody
- Deep Fake Videos
- Politics

Things are so bad the Government's energy is centered on protecting itself and critical infrastructure.

THE BUSINESS OF CRIME

The business of cybercrime is not unlike a typical start-up business model. There's a product with a clear value proposition, integrated marketing campaigns, customer support services, risk and rewards analysis, research and development and more. There are even Black Friday deals for criminals on the dark web.

WAWA HACK

Brand NEW Huge 30M+ pcs Nationwide
"BIGBADABOOM-III" BREACH at JOKER's STASH!

Brand NEW Huge **30M+ pcs** Nationwide Breach
30.000.000+ Perfect Pure Fresh TR2+TR1 Dumps
40+ US States
31.000+ Different Bins
more than **1M pcs** of EU/ASIA/ARABS/EXOTIC bins (100+ Different Countries)

BIGBADABOOM-III-EU-part1 (BBB3 BREACH) **EU/ASIA/WORLD TR1+TR2/TR2, HIGH VALID 90-95%**, uploaded 2020-01-27
BIGBADABOOM-III-US-part1 (BBB3 BREACH) **USA by STATE/CITY/ZIP TR1+TR2/TR2, HIGH VALID 90-95%**, uploaded 2020-01-27
BIGBADABOOM-III-US-part2 (BBB3 BREACH) **USA by STATE/CITY/ZIP TR1+TR2/TR2, HIGH VALID 90-95%**, uploaded 2020-01-27
BIGBADABOOM-III-US-part3 (BBB3 BREACH) **USA by STATE/CITY/ZIP TR1+TR2/TR2, HIGH VALID 90-95%**, uploaded 2020-01-27

Be READY for the BIG-BADA-BOOM! Exclusively ONLY at JOKER's STASH!

ALL STUFF WILL BE AVAILABLE AT
11:00 PM (evening update) New York City Time, Monday, January 27

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*

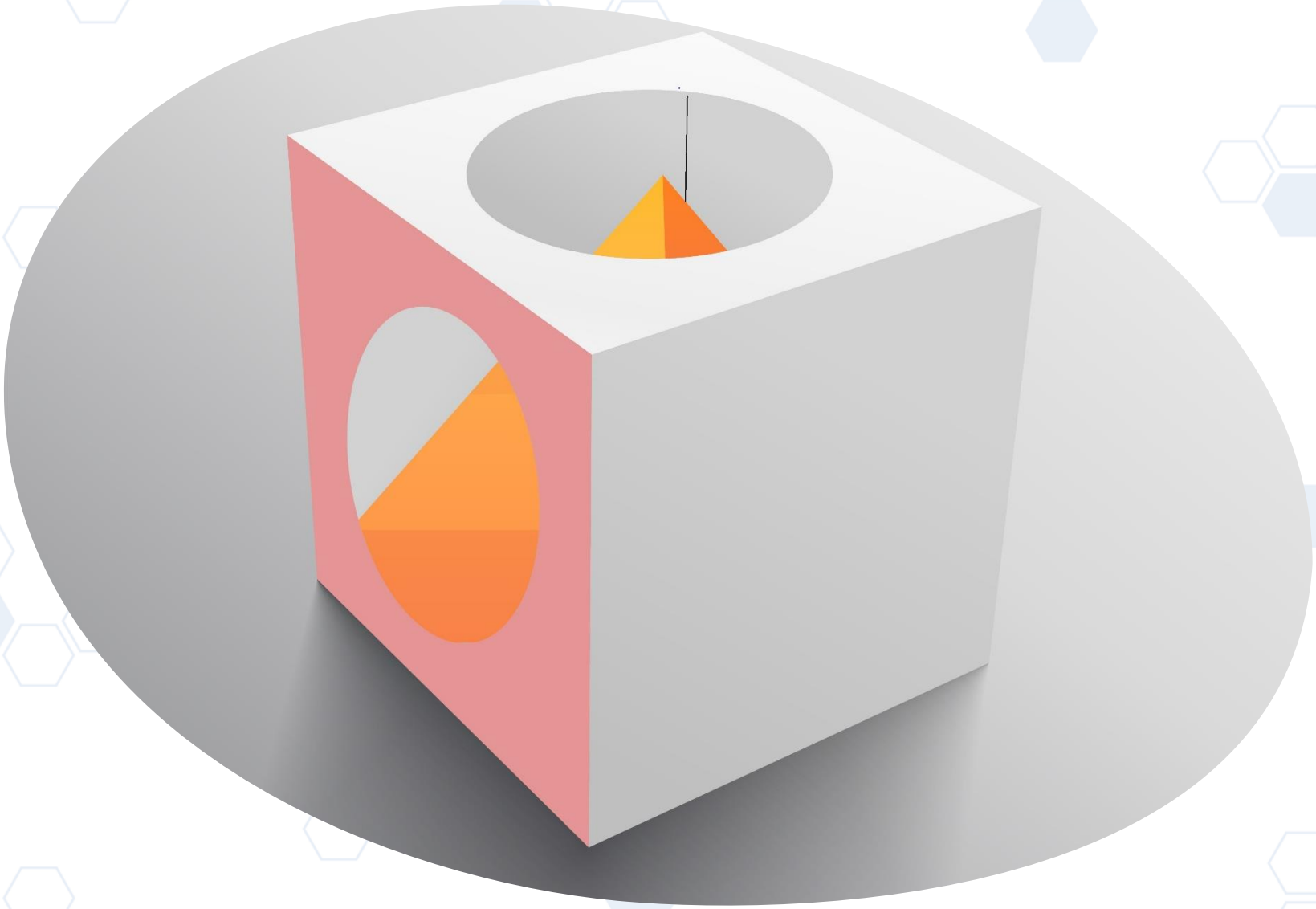
Physical breach is not necessary to undermine confidence, question integrity or minimize access

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*

RISK MANAGEMENT

Risk management is a fundamental component of any successful organization. The primary function of risk management as a whole is to allow business leaders to determine the best course of action based on the probability of a given outcome and the possible determinants of that decision.



Perspective

A particular attitude toward, or way of, regarding something; a point of view.

CYBERSECURITY COMPANIES

FireEye, a cybersecurity company that defends third-parties worldwide, announced on December 8th that they had suffered a data breach. Hackers accessed tools the company uses for penetration testing against its clients' security. FireEye uses these tools to simulate a real attack by hackers.

According to FireEye, this attack was highly-targeted and sophisticated and likely came from a state-sponsored hacker.

INFORMATION TECHNOLOGY COMPANIES

The SolarWinds attackers ran a master class in novel hacking techniques. They modified sealed software code, created a system that used domain names to select targets and mimicked the Orion software communication protocols so they could hide in plain sight.

And then, they did what any good operative would do: They cleaned the crime scene thoroughly so responders can't prove definitively who was behind it.

SOCIAL MEDIA COMPANIES

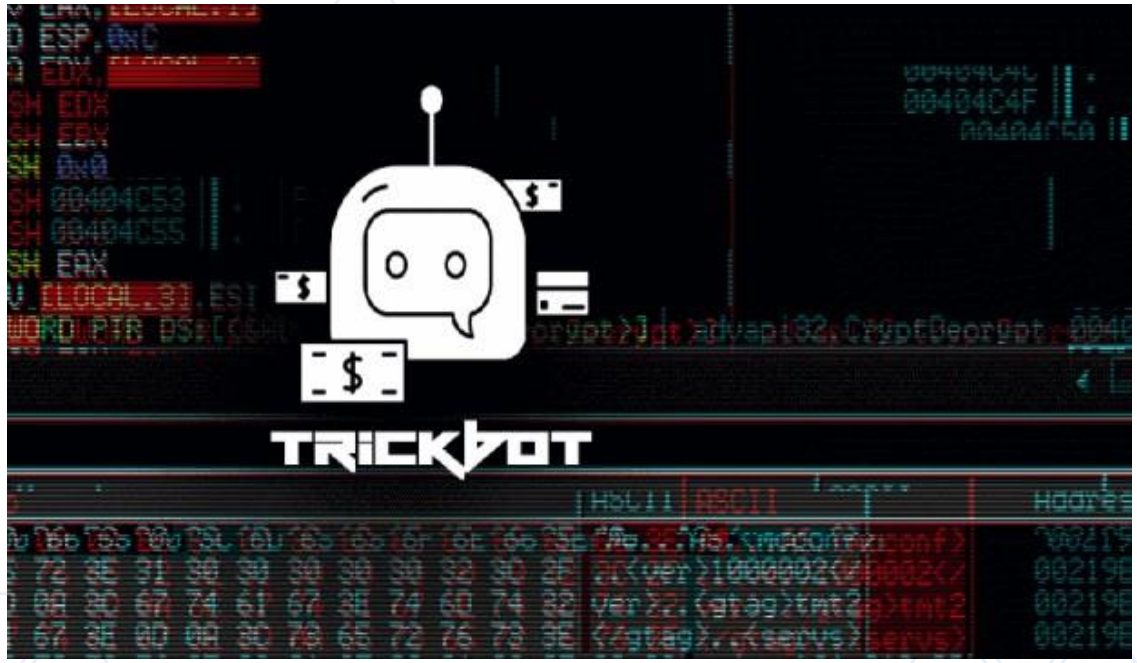
On December 14th, Google experienced an outage that prevented users from accessing various services. The outage lasted for more than an hour and caused a storm of social media.

The potential hack against Google has affected nearly 70 million users across various services.

RISE OF THE BOTS

Trickbot was used in an attack against a major health-care provider, Universal Health Services. The company runs more than 400 facilities across the United States and Britain.

The attack forced personnel to resort to manual systems and paper records.



In 2020, Microsoft took action against the Trickbot botnet. Microsoft worked with telecommunications providers around the world to disrupt key Trickbot infrastructure. Operators will no longer be able to use this infrastructure to distribute the Trickbot malware or activate deployed payloads like ransomware.

IMPACT OF PANDEMIC

The coronavirus pandemic has been connected to a 238% surge in cyberattacks against banks. Close to a third -- 27% -- of all cyberattacks target either banks or the healthcare sector.

According to Malwarebytes, **20% of companies said they faced a security breach specifically as a result of a remote worker**, and 24% spent unbudgeted dollars on cybersecurity breaches or malware attacks.

It's estimated that **one in 36 mobile devices have high-risk applications installed.** When employees mix work and leisure on their device, these vulnerabilities provide potential openings for attackers to steal credentials.

The 2020 Verizon Data Breach Investigation report highlights a **year-over-year two-fold increase in web application breaches to 43%. Stolen credentials were used in over 80% of these cases.**

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 to build a culture that continuously seeks **visibility of assets**, **understanding of interdependencies** and redefines **each person’s role.**
- The investment has to be put into community and stakeholder education.

SUPPORTING A SECURE ENVIRONMENT

Many operators have still not taken adequate measures to protect systems. As an example: Not employing role-based access control for employees multiplies their risk by giving vendors and partners high-level system access.

Zero Trust - or earned trust, access model needs to be put in place. Start by calculating the potential harm of compromised. Map out functional zones and implement segmentation and access controls to limit the scale of a breach.

User and Entity Behavior Analytics - systems should be installed to detect and respond rapidly to any abnormal behavior that threatens safe operations.

Educate - Cybersecurity awareness programs, cyberliteracy programs and cyber hygiene training are not IT training courses. They should be a refresh of the organization's culture.

Provide all staff a reason to care.

QUESTIONS

Michael Echols

CEO, Max Cybersecurity

mechols@maxcybersecurity.com

Connect on LinkedIn