Michael Best

Privacy/Cybersecurity

Ryan T. Sulkin

Michael Best

Not Ghosts

- $2.1 Billion—estimated annual cost of internet data breaches by 2019
- The average total cost of a data breach is $3.86 million, the average global possibility of a breach in the next 24 months is 27.9%, and the average breach cost reduction for organizations using security automation is $1.55 million
- 56% of 1,379 incidents with specific malware functionality were ransomware
- 668 breaches compromised 22,408,258 records between January 1 and July 2, 2018

How does it happen?

Target: HVAC service provider

Equifax: Failure to patch vulnerability

Anthem: A user within one of Anthem's subsidiaries reportedly opened a phishing email containing malicious content. Opening the email permitted the download of malicious files to the user's computer and allowed hackers to gain remote access to that computer and at least 90 other systems within the Anthem enterprise, including Anthem's data warehouse.

Heartland: SQL injection techniques were used to install spyware onto Heartland's data systems and monitor credit card transactions.

Marriott: Starwood system infiltrated; potentially years before deal closed

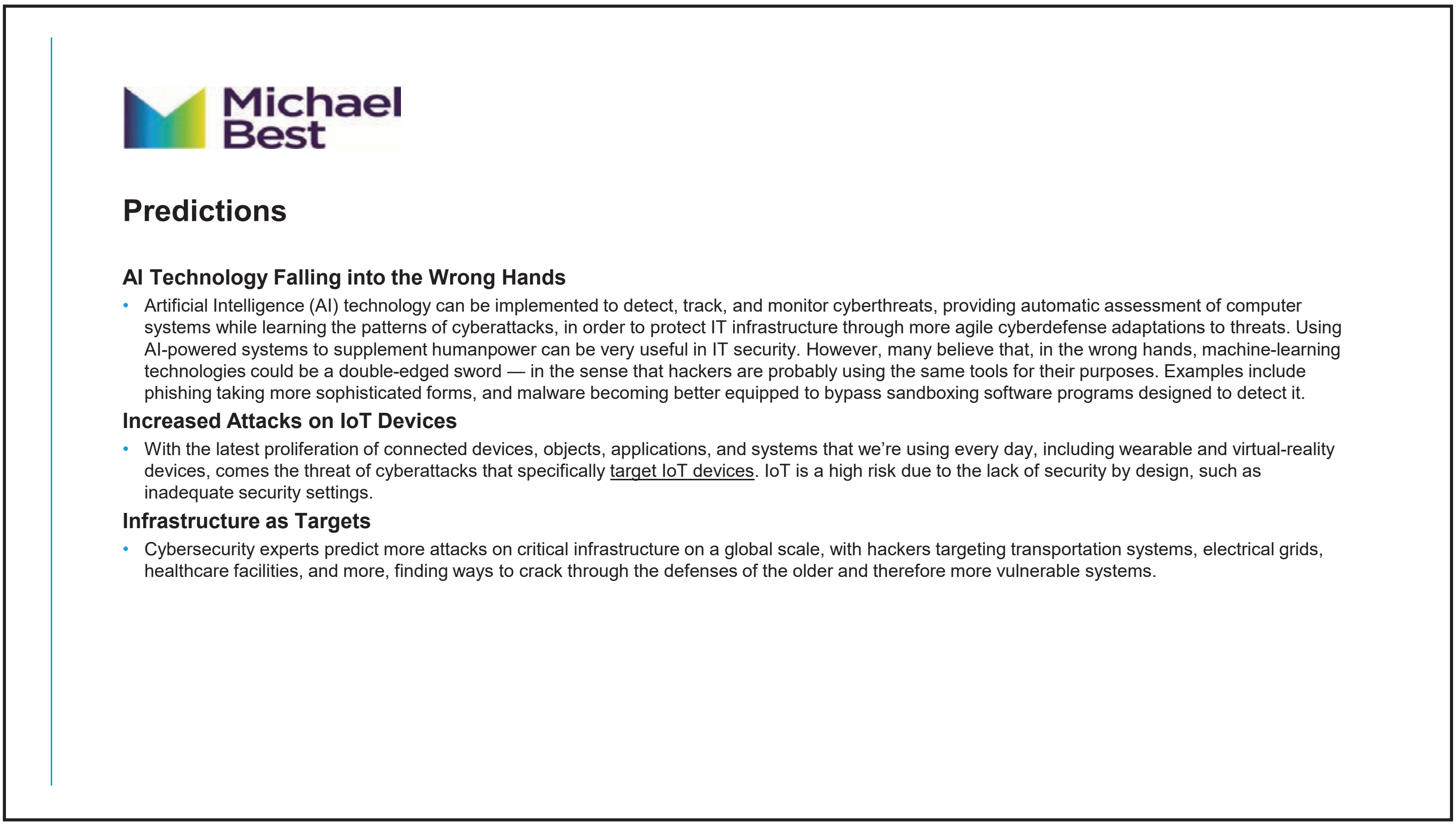
Predictions

Massive Data Breaches Will Continue

- More massive data breaches affecting large companies.

Ransomware Attacks Targeting the Cloud

- Ransomware, which is malware that uses encryption to lock down computer files, is a popular hacker weapon because of its relative simplicity, and because of its lucrativeness, charging money, often demanded in the form of hard-to-trace cryptocurrency, to unlock hostage data.
- New strains multiply quickly, and often, too. Some particularly vicious strains, such as WannaCry, NotPetya, and Bad Rabbit, wreaked havoc last year, compromising hundreds of thousands of computers and impacting businesses big and small across many industries. Maersk and FedEx, for instance, reported millions of dollars in damage due to the NotPetya ransomware attacks in 2017.
- Cloud-computing is a target.



Michael Best

Predictions

AI Technology Falling into the Wrong Hands

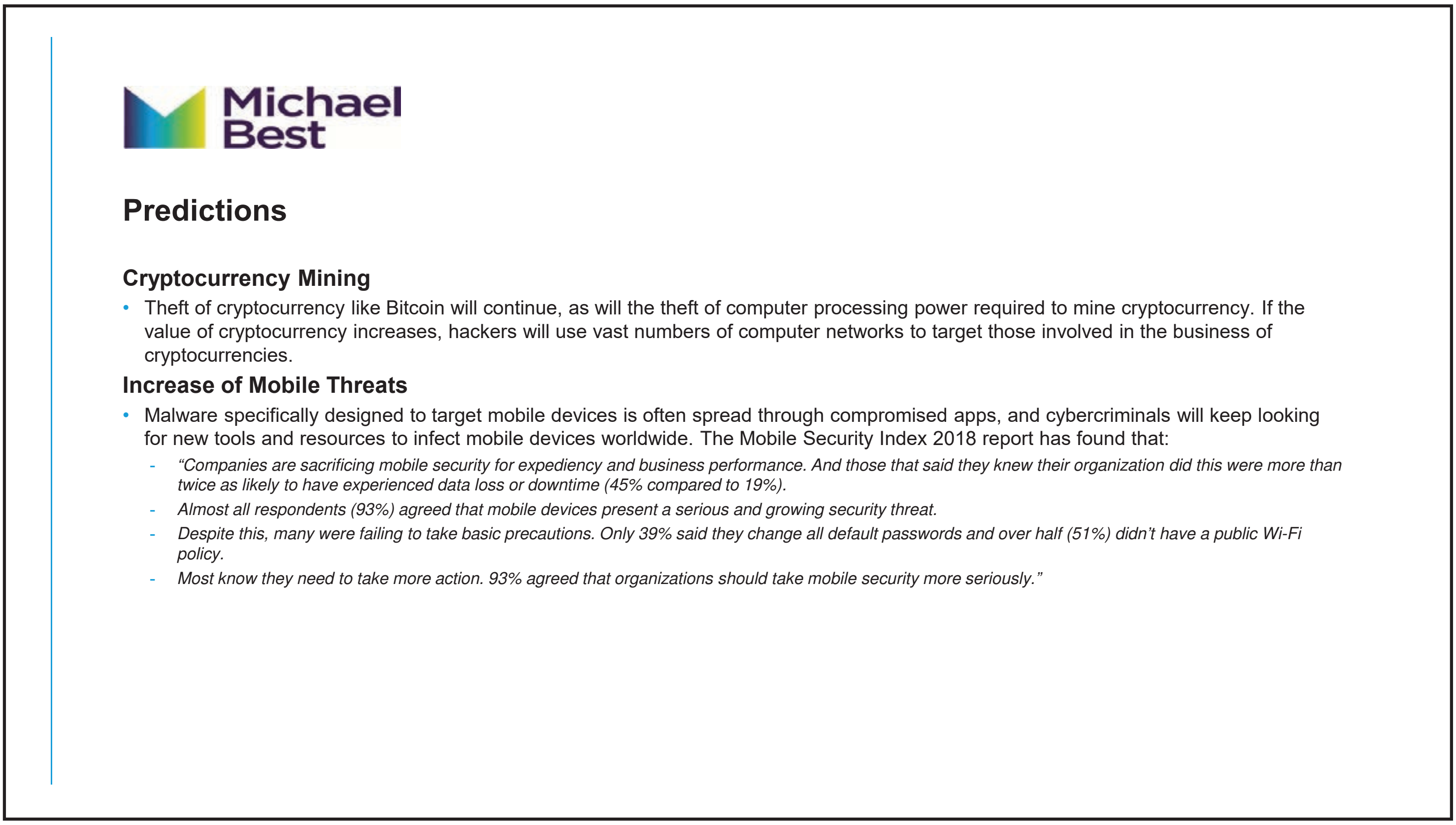
- Artificial Intelligence (AI) technology can be implemented to detect, track, and monitor cyberthreats, providing automatic assessment of computer systems while learning the patterns of cyberattacks, in order to protect IT infrastructure through more agile cyberdefense adaptations to threats. Using AI-powered systems to supplement humanpower can be very useful in IT security. However, many believe that, in the wrong hands, machine-learning technologies could be a double-edged sword — in the sense that hackers are probably using the same tools for their purposes. Examples include phishing taking more sophisticated forms, and malware becoming better equipped to bypass sandboxing software programs designed to detect it.

Increased Attacks on IoT Devices

- With the latest proliferation of connected devices, objects, applications, and systems that we're using every day, including wearable and virtual-reality devices, comes the threat of cyberattacks that specifically target IoT devices. IoT is a high risk due to the lack of security by design, such as inadequate security settings.

Infrastructure as Targets

- Cybersecurity experts predict more attacks on critical infrastructure on a global scale, with hackers targeting transportation systems, electrical grids, healthcare facilities, and more, finding ways to crack through the defenses of the older and therefore more vulnerable systems.



Michael Best

Predictions

Cryptocurrency Mining

- Theft of cryptocurrency like Bitcoin will continue, as will the theft of computer processing power required to mine cryptocurrency. If the value of cryptocurrency increases, hackers will use vast numbers of computer networks to target those involved in the business of cryptocurrencies.

Increase of Mobile Threats

- Malware specifically designed to target mobile devices is often spread through compromised apps, and cybercriminals will keep looking for new tools and resources to infect mobile devices worldwide. The Mobile Security Index 2018 report has found that:
  - *"Companies are sacrificing mobile security for expediency and business performance. And those that said they knew their organization did this were more than twice as likely to have experienced data loss or downtime (45% compared to 19%).*
  - *Almost all respondents (93%) agreed that mobile devices present a serious and growing security threat.*
  - *Despite this, many were failing to take basic precautions. Only 39% said they change all default passwords and over half (51%) didn't have a public Wi-Fi policy.*
  - *Most know they need to take more action. 93% agreed that organizations should take mobile security more seriously."*