CRITICAL INFORMATICS

Our stuff keeps your stuff from becoming their stuff
UW Tech Connect
March 13, 2018

Trends In Information Security
Preparing for an animated future
Outcomes to Avoid

- Records Breach: ~$150/record
- Theft: $75K-$1.2M in our region, multiple millions elsewhere
- Disruption: Loss of business continuity or operating capacity, loss of life for critical services
Leaning Into OSINT

Trends emerge, which lend themselves to prediction, or at least noticing which way the wind is starting to blow.
Recent Public Sector Events

Montgomery County Public Schools Says It Was Target of Cyberattack

Electronic disruption lasted three days, district spokesman says

Man Behind 911 Call System 2016 Cyberattack Sentenced to Probation

Meetkumar Desai pleaded guilty in August to felony count of solicitation to commit computer tampering

Cyber-criminals attack Atlanta, Fulton, and Clayton school districts, paychecks stolen

October 05, 2017

City of Englewood, Colo. hit with ransomware

The attack left the city's civic center unable to process credit cards and the city's library unable to place items on hold or accept late fines, according to an Oct. 4 press release.
Ransomware

Ransomware for robots is the next big security nightmare

Researchers found they were able to infect robots with ransomware; in the real world, such attacks could be highly damaging to businesses if robotic security isn’t addressed.

By Danny Palmer | March 9, 2018 -- 15:47 GMT (07:47 PST) | Topic: Security

5 ransomware as a service (RaaS) kits

Connected Cars are vulnerable to Ransomware Attacks

Medical Devices Hit By Ransomware For The First Time In US Hospitals
Cryptocurrency Mining

Low-Risk for organized crime
Uses existing botnets
Becoming legitimized
Operational Continuity Threat
Better than ransomware
IoT Weaponization

- Not secured when deployed
- If exposed to the Internet, immediate takeover
- Mirai, Reaper, DoubleDoor
- Used for DDOS, and TBD
What’s Going Wrong Here?

- **Manufacturers** – do not produce products that are certified as free of known security defect
- **Procurement** – does not require any attestation of product security as a requirement for purchase
- **Integrators** – do not install products with security controls
- **Operations** – does not address roles and responsibilities delineation for security
Lawsuits

Class-action cyber attack lawsuit against Banner Health may be the first of many


Yahoo sued for gross negligence over cyber-attack that exposed 500 million accounts


August 16, 2016

After the breach: Settlement expected for 50M Home Depot customers

https://www.scmagazine.com/after-the-breach-settlement-expected-for-50m-home-depot-customers/article/529135/

Threats of Litigation After Data Breaches at Major Law Firms

March 30, 2016

Shareholders Sue Companies For Lying About Cyber Security

Another key area to focus on is litigation exposure. While this area of law is still developing, breaches can give rise to consumer litigation, securities fraud litigation, even liability for corporate directors under Delaware law.

[...]

The markets are becoming much more sophisticated in their understanding of the financial consequences of breaches that result in the loss of key intellectual property, and legal exposure is also expanding rapidly, especially on the consumer front. Some courts are starting to permit consumers to bring cases based on the fear of fraud that they suffer after their data is stolen—even without being able to show that anybody has actually tried to use their data. As we start to see share prices drop after news of previously undisclosed breaches emerges, I think we will be seeing more securities fraud suits as well.

Nation-State Collateral Damage

“The superficial resemblance to Petya is only skin deep. Although there is significant code sharing, the real Petya was a criminal enterprise for making money. This is definitely not designed to make money. This is designed to spread fast and cause damage, with a plausibly deniable cover of ‘ransomware.’”
The Third Party Microscope

Verizon & 500,000 Vehicle Tracking Accounts Exposed On Misconfigured AWS S3

Opus & Ponemon Institute Announce Results of 2017 Third Party Data Risk Study: 56% of Companies Experienced Data Breach, Yet Only 17% are Prepared to Mitigate Risk

Extreme Vetting: Evaluating The Security Posture Of Third-Party Vendors
A Spyware Company Audaciously Offers ‘Cyber Nukes’

“This ability enables an agency to instantly disable or destroy a target. Cyber strike capability is an ‘always online weapon’ that can be fired at any IP connected terminal with power to disable or destroy a target permanently,” a copy of the brochure reads, referring to Aglaya’s self-described ‘Cyber Strike’ product.

“This weapon is comparable to a Nuclear Strike that can destroy city wide Cyber infrastructure or render a county wide IP communications ineffective,” the brochure adds.

Gigantic DDOS

Memcached Amplification Attack Breaks New DDoS Record At 1.7 Tb/s

Arbor believes that we’ve entered a new era in which Tb/s DDoS attacks will be common, whether it’s through memcached server vulnerabilities or through other vulnerabilities attackers may be able to find later.
Hardware Vulnerabilities

Meltdown-Spectre: Now the class action suits against Intel are starting to mount up

"One of the problems with Spectre is that it's completely silent," Evtyushkin said. "You don't see anything happening. Compared to traditional attacks, where an application usually crashes and you can see the damage, with microarchitecture attacks you won't see it or know it happened."

Surveillance, Privacy, and Encryption

Tension between ad revenue and product companies
GDPR and the right to data removal
Disinformation, propaganda, and voter manipulation
US wants private sector cooperation w/foreign govt
data requests
Role of local law enforcement

The CLOUD Act: A Dangerous Expansion of
Police Snooping on Cross-Border Data

BY CAMILLE FISCHER  |  FEBRUARY 8, 2018

Not Everything is Bad… We Think

AI, ML, and Security Automation
Not-So-Crazy Predictions

SADLY
• DDOS will become a more prevalent (and effective) extortion tool
• Ransomware will affect transportation, manufacturing, and health sectors
• Our economy will be poked by a nation-state actor
• Government surveillance will increase
• The 2018 election will be chaos
• Extortion against a hospital will result in a death

BUT ALSO
• Boards of Directors will treat "cyber" as a business risk
• Automation with human oversight will start to help
• Security will become a competitive differentiator
THANK YOU

Mike Hamilton
Michael.Hamilton@criticalinformatics.com
@critinformatics – Company Tweets
@seattlemkh – Unvarnished Opinions

The IT Security News Blast
https://criticalinformatics.com/resources/it-security-news/
Critical Informatics
Our stuff keeps your stuff from becoming their stuff

info@criticalinformatics.com

Twitter
@seattlemkh
@critinformatics