Cybersecurity – No Need to Panic
A Practical Approach to Protecting Yourself

Tom Clark
Chief Information Officer
November 7, 2018
Remember This One?

Clip is located at https://www.youtube.com/watch?v=KXzNo0vR_dU
So What Changed? What’s the Problem Now?

- There is a hacker attack every 39 seconds, affecting one in three Americans each year.

- 95 percent of breached records came from three industries in 2016: Government, retail, and technology.

- Since 2013 there are 3,809,448 records stolen from breaches every day, 158,727 per hour, 2,645 per minute and 44 every second of every day.

(https://www.cybintsolutions.com/cyber-security-facts-stats/)

- According to the 2018 Verizon Data Breach Report, 76% of breaches were financially motivated.

- Almost three-quarters (73%) of cyberattacks were perpetrated by outsiders.

- Members of organized criminal groups were behind half of all breaches, with nation-state or state-affiliated actors involved in 12%. Over a quarter (28%) of attacks involved insiders.

(https://enterprise.verizon.com/resources/reports/dbir/)
Why Now?

It is cheaper and easier to do. You don’t need to be highly educated or technical.

Cryptocurrency and dark web marketplaces make it easy to convert stolen data to cash and goods.

Connected networks make it easy to cross global boundaries where law enforcement is weak or absent.

There are literally billions of targets.
Dark Web Marketplaces
What are the risks?

• Compromise
• Destruction/Loss
• Integrity
What is the one thing I need to do to protect myself?

In spite of what security vendors may tell you, there is no silver bullet.
There is no shortage of solutions. Approximately $1 trillion is expected to be spent globally on cybersecurity from 2017 to 2021. https://www.cybintsolutions.com/cybersecurity-facts-stats/  

Security marketing causes a lot of anxiety but usually provides no real relief. Answers are typically heavily biased toward individual products. 

Source: https://www.cbinsights.com/
How does a business leader sort through the noise.

- Understand what is valuable and where it is stored.
- Focus on the fundamentals.
- Look for a layered approach.
What data is valuable and where is it?

- Transactional Systems
- Financial
- Health
- Identity
- Trade Secrets
Focus on the Fundamentals

• Isolate sensitive data.
• Keep systems current and patched.
• Enforce good e-mail practices.
• Restrict access to sensitive information.
• Encrypt sensitive data.
• Use strong passwords and multi-factor controls.
• Avoid high-risk websites and untrusted mobile applications.
• Insist on qualified personnel and structured controls. Call experts when necessary.
Adopt a Layered Defense Model

Are non-technical controls important?

- Manual Verification Processes
- Training
- Culture
Five Questions to Ask Your Technical Team

• Do you understand what my sensitive data is and where it is stored?

• Can you describe the different layers of your information security strategy?

• How do you keep our systems patched with the latest software updates?

• How would you know if we were attacked?

• What would happen if we were hacked?
How can I learn more?

SANS Institute
• [https://www.sans.org/security-resources/](https://www.sans.org/security-resources/)

NIST – Computer Security Resource Center
• [https://csrc.nist.gov/](https://csrc.nist.gov/)

DEFCON
• [https://www.defcon.org/](https://www.defcon.org/)

BlackHat
• [http://blackhat.com/](http://blackhat.com/)

ISACA
• [https://www.isaca.org/pages/default.aspx](https://www.isaca.org/pages/default.aspx)