ThreatAdvice

CYBERSECURITY BASICS AND RECENT TRENDS

Joe McEnerney

May 26, 2021

CYBERSECURITY BASICS

WHAT YOU NEED TO KNOW AND WHY IT MATTERS

NXTsoft

ThreatAdvice by NXTsoft

> There are only two types of companies: Those that have been hacked, and those that will be.

Robert Mueller, FBI Director, 2012

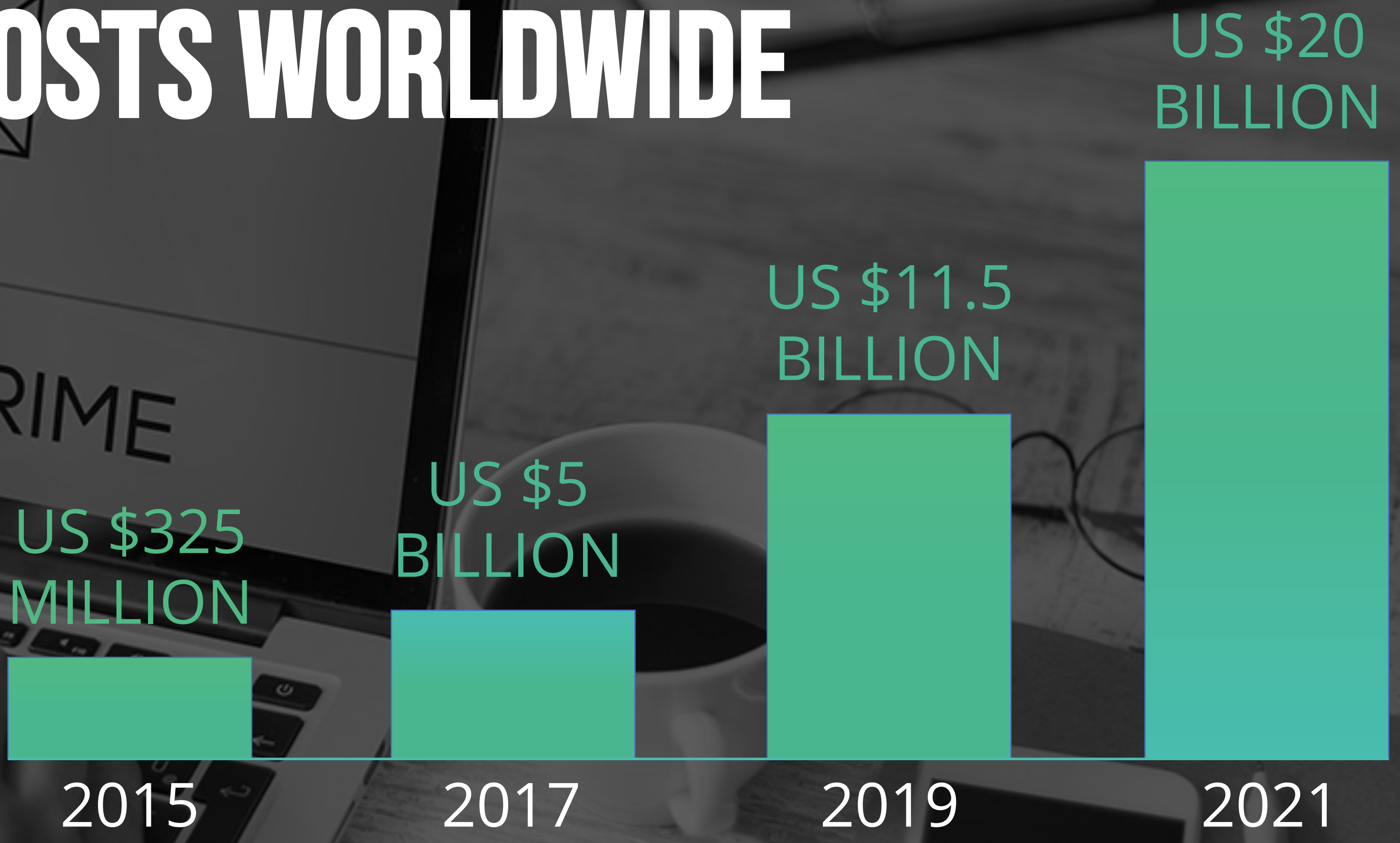
Conclusion: The bad guys are “winning the cyber battle”

Threats in Cyberspace

- Distributed Denial of Service
- Crypto-jacking
- Wire Transfer Fraud
- Phishing and Spear phishing
- Smishing attack by text or SMS

TYPES OF ATTACKS

GROWTH IN RANSOMWARE DAMAGE AND COSTS WORLDWIDE



WHAT IS A LAYERED APPROACH TO SECURITY?

Think about your home and property....

The walls, roof, foundation, windows and doors serve as the first layer of protection to the outside world.

WHAT IS A LAYERED APPROACH TO SECURITY?

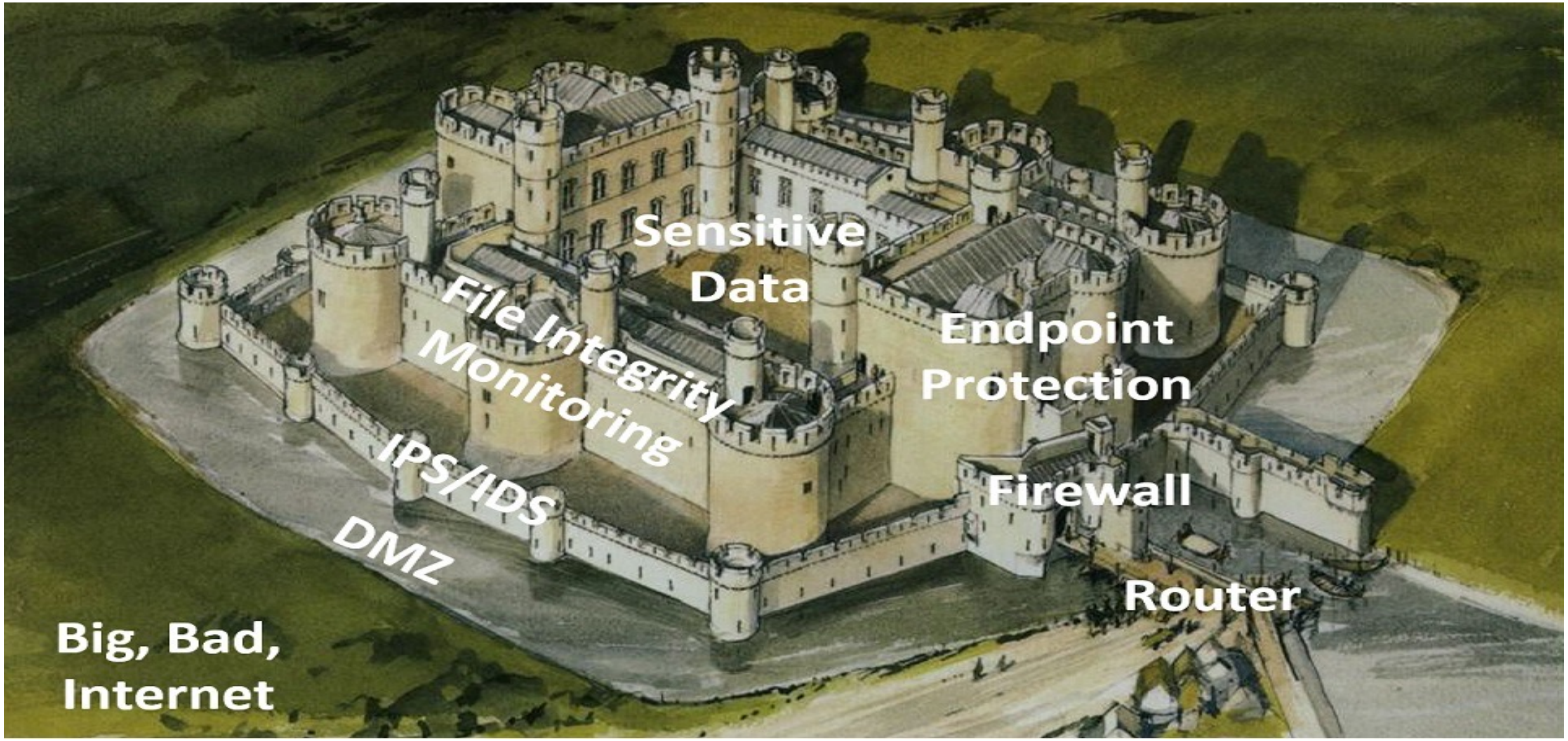
Door locks, window locks and deadbolts are a second layer

For some people, that's considered adequate protection, but for many others, more layers are applied.

WHAT IS A LAYERED APPROACH TO SECURITY?

Many homes are equipped with security systems that both alert home owners of intruders and deter criminals for attempting access.

PROTECT YOUR COMPANY'S DATA AS YOU WOULD PROTECT YOUR CASTLE



ADDITIONAL STEPS FOR DATA PROTECTION

Cybersecurity Checklist

Have Institution wide Cybersecurity Policies and Procedures in place

Employ a SIEM coupled with a Security Operations Center (SOC)

Employ two-factor password authentication and encourage employees to routinely change passwords

Implement and employee education and awareness training program

Employ next generation end point protection software and firewall

CYBERSECURITY CHECKLIST

Items To Address In Addition To Employee Education and Awareness

Immediately update all software patches

Back-up data routinely and have an action plan in case of a data breach

Treat cybersecurity as a business responsibility, not just an IT responsibility.

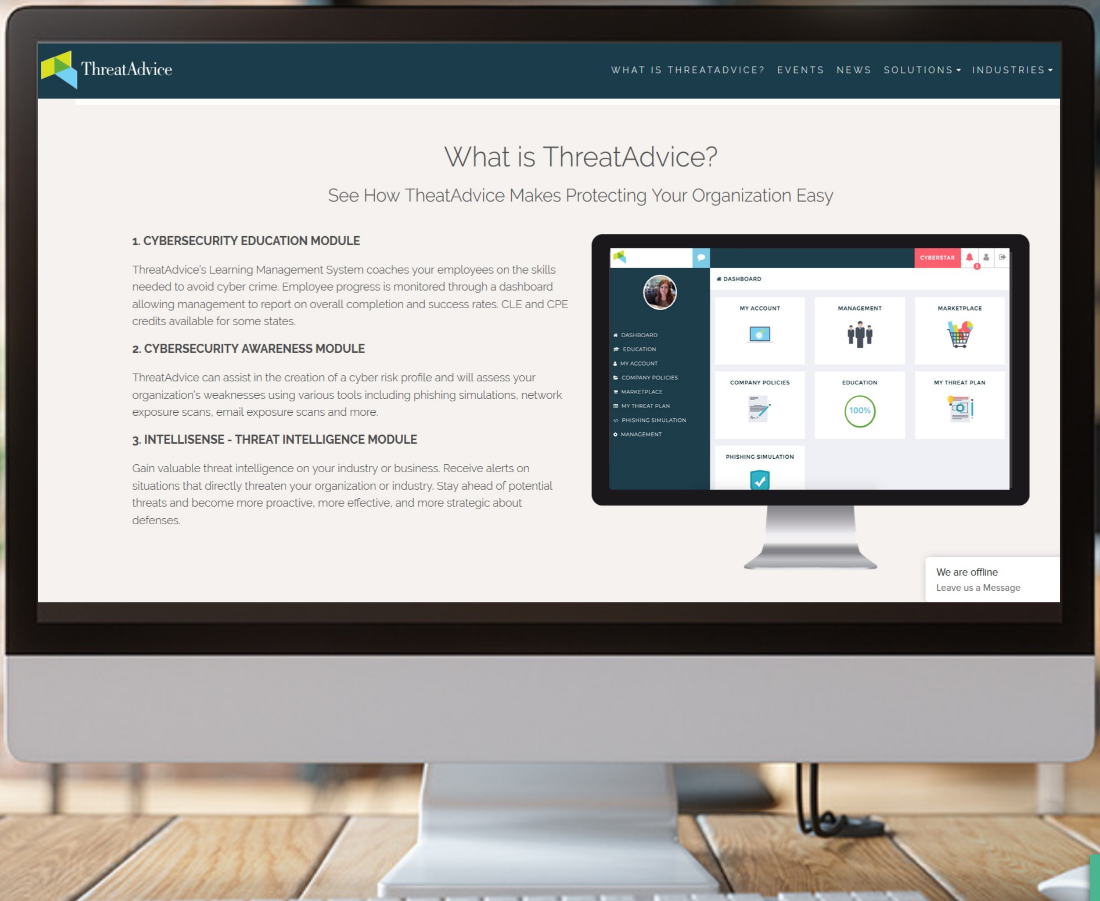
Purchase Cyber insurance

Don’t get lazy

HOW TO MAKE YOUR EMPLOYEES CARE ABOUT CYBER TRAINING

- **Emphasize the Importance of Understanding Risks.** Detail the consequences and losses the organization will face if a cyber incident occurs and share that information with employees.
- **Share News of Breaches in your Industry.** When another companies in your industry experiences a breach, make sure your employees know about the breach and its results.
- **Enact Information Security Policies.**
- **Use Engaging Training Material**. Use material that both teaches your employees and holds their attention.
- **Incentivize Cybersecurity Education**. Gift cards and days off. Recognize employees who exceed expectations.
- **Make it Fun!** Incorporate incentives into competitions or enact some other type of gamification to keep employees interested and continuously reviewing their education.

QUESTIONS?



What is ThreatAdvice?

See How TheatAdvice Makes Protecting Your Organization Easy

1. CYBERSECURITY EDUCATION MODULE

ThreatAdvice's Learning Management System coaches your employees on the skills needed to avoid cyber crime. Employee progress is monitored through a dashboard allowing management to report on overall completion and success rates. CLE and CPE credits available for some states.

2. CYBERSECURITY AWARENESS MODULE

ThreatAdvice can assist in the creation of a cyber risk profile and will assess your organization's weaknesses using various tools including phishing simulations, network exposure scans, email exposure scans and more.

3. INTELLISENSE - THREAT INTELLIGENCE MODULE

Gain valuable threat intelligence on your industry or business. Receive alerts on situations that directly threaten your organization or industry. Stay ahead of potential threats and become more proactive, more effective, and more strategic about defenses.

We are offline
Leave us a Message

JOE MCENERNEY

Jmcenerney@nxtsoft.com
(251) 610-3334

nxtsoft.com/security