Effectively Managing Cyber Security for the Enterprise

In a complex enterprise that faces an ever changing threat landscape, the team in charge of cyber security may find it difficult to know where to focus limited resources. Areas such as firewalls and operating system updates are obvious priorities. But what else?

Top 5 Security Threats

Hackers of today are exhibiting more patience, planning, and boldness than ever before.

Top 5 Smart Moves

Enterprises can make smart, high-impact security moves to avoid critical threats.

Threat #1

Hackers will continue to attack your organization through your employees

91% of targeted attacks involved spear phishing emails

TOP THREE TACTICS

- Social Media
- Malicious Email
- Website Malware

Threat #2

Enterprises will continue to underestimate malicious insiders

56% of executives say their most serious fraud was due to a privileged user

Threat #3

Cyber attacks will in some cases cause physical damage

Stuxnet (2010) was first known case of a cyber attack causing physical damage

Many enterprises have NOT secured cyber-physical and embedded systems

Threat #4

Advanced Persistent Threats (APTs) launch subtle, long-term enterprise attacks

The org that launched Operation Shady RAT IN 2006 successfully penetrated:

71 COMPANIES

ACROSS

31 INDUSTRIES

Security industry experts are realizing APTs are more common than previously thought

Threat #5

Ransomware will appear on mobile devices, IoT & networks

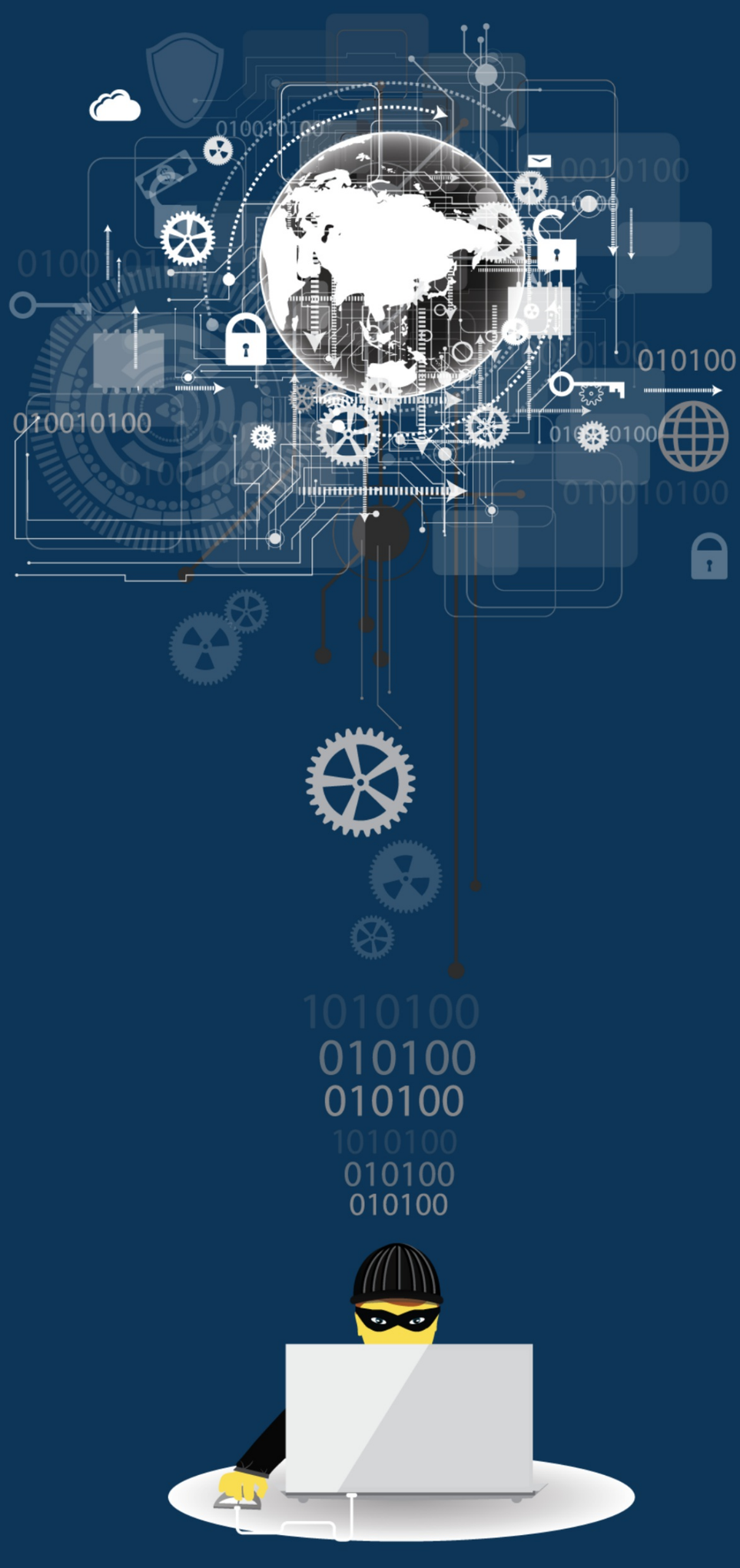
IT DECISION MAKERS STATED:

20% said ransomware is NOT part of their security strategy

22% are not confident with the technology they have in place to combat ransomware

24% have technology in place to combat ransomware, but they are more concerned with employees adhering to security policies

Forrester Research predicts in 2016, the world will see some of the first ransomware attacks on wearable and medical devices impacting the enterprises that manufacture them



Smart Move #1

Update your security policy to communicate data security expectations

AREAS TO CONSIDER:

- Transporting Sensitive Info
- Use of Public Wi-fi
- Working from Home
- Use of External Storage

Smart Move #2

Train employees using security scenarios comprehension testing

23% will open an email that allows an attacker to begin attacking a network

Smart Move #3

Control worker access and track digital footprints

MONITOR THE FOLLOWING:

- Device IPs
- Critical File Access
- Manual Package Updates
- Config File Changes

Smart Move #4

Assess the security of vendors and third-party software

ASK YOUR VENDOR:

- How is security integrated into the product development lifecycle?
- Is the security of the software tested internally and/or externally?
- What's the disaster recovery plan?

Consider random vendor audits for compliance

Smart Move #5

Fortify your defenses for mobile, IoT, and other devices

Inventory all devices interacting with your network & check for security updates reguarly

WEI Dedication meets innovation.

NEXT STEPS

Free Security and Threat Prevention Assessment

Before investing in software or hardware security solutions, sign up for a free Security and Threat Prevention Assessment from WEI.

(800) 296-7837 info@wei.com 24/7 www.wei.com

Sources

-IDG TechPulse poll of 116 ITDMs on March 22, 2016, research commissioned by Worldcom Exchange, Inc.
-2015 Data Breach Investigations Report (Accessed January 6, 2016). Verizon. Web.
-TrendLabs APT Research Team. Spear-Phishing Email: Most Favored APT Attack Bait (2012): 1. Trend Micro Incorporated.
-Zetter, Kim. A Cyberattack Has Caused Confirmed Physical Damage for the second Time Ever (January 8, 2015). Wired Magazine.
-Alperovitch, Dmitri. Revealed: Operation Shady RAT (White Paper, 2011). McAfee.
-Hayes, Nick, Holland, Rick, et al. Predictions 2016: The C-Suite and Cybersecurity (November 12, 2015). Forrester Research.