Black Hat Web Series
BleedingBit and IOT devices
Future Workplace

Driven by changes in how people are working – and what they need from the office environment

Traditional office

Emerging office

- Agile workspaces for individual productivity
- More informal meeting areas for co-creation, collaboration
- Interactive conference rooms for meetings, collaboration
- Open environment with neighborhoods
- Integrated communal spaces for socialization, play, wellness

Work outside the traditional office increasing

Home  Cafe/public space  Airplane
Today’s Meeting Room Technology

The market is busy innovating, and technology options are multiplying

- Simplified Projection
- Team collaboration devices

Barco Clickshare, Intel Unite, SmartBoard, Cisco Spark, MSFT Surface Hub
The Changing Threat Landscape

Commercialization of attack software

Black-hole Exploit Service Command Console

Autosploit loader
Required Next Steps

- Procure devices with **remote management** in mind
- Insist on **common interfaces** & management tools
- Own organizational responsibility
- Establish IoT security policy appreciating diversity of endpoints

Plan to Manage & Control
Print jobs on network
Android July 2019 Security Update Patches 33 New Vulnerabilities

Amazon Admits Alexa Voice Recordings Saved Indefinitely

Print-related data breaches affected 60% of businesses last year

By Anthony Spadafora  February 12, 2019  Internet

Print is a growing security concern
NSA Presentation at RSA 2018

- 93% of 2017 incidents preventable with best practices
- In 2018, NSA stated 90% of cyber incidents due to human error

GOOD CYBER HYGIENE
80% of cyber attacks preventable with basic cyber hygiene
1. Every purchase decision is a SECURITY decision

2. CIO & CISO must get involved early in all endpoint procurement to ensure and drive security requirements into the endpoint procurement decisions

3. On-going assessment and monitoring of endpoint risks

4. Increase data controls for endpoint devices

5. Data breach monitoring and reporting for all endpoints

6. On-going evaluation and monitoring of endpoint protections deployed

7. Treat endpoint devices as the first line of defense

8. Include all endpoint devices in your policies and security action plans

Key Takeaways

Assess risk

Build controls

Monitor controls
Thank you

Ronald.Chestang@hp.com

www.hp.com/thewolf
www.hp.com/reinventsecurity