



**Eric Thebe** CISM, GCIAH, CEH

Technical Consultant CEMA

April 26-28, 2017

Member of ISSA (*Information Systems Security Association*)





# HP JetAdvantage Security Printing

## **Can A Printer Compromise Your Business?**





# What are the top printing security concerns?

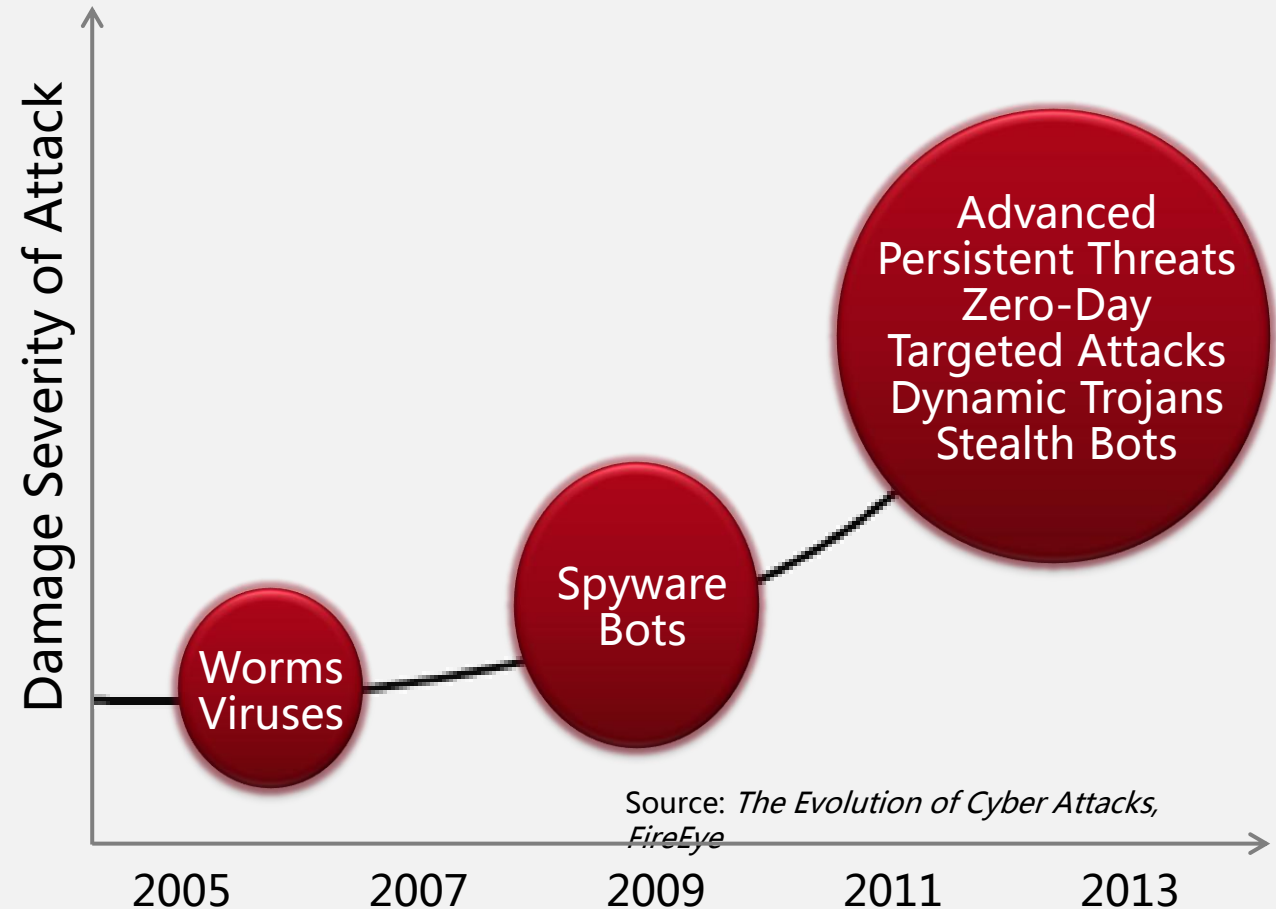
- 1) **Exposure of data** in transit
- 2) **Company' s ability to identify a security breach** from printers
- 3) **Exposure of documents** left in the output tray
- 4) **Unauthorized use** of printer features
- 5) **Remote employee' s** use of home printers
- 6) **Exposure of device** network settings or ports
- 7) **Threat of outside malicious access** to network through printers



# Landscape Changes: Cyber Attacks and Motives are Evolving

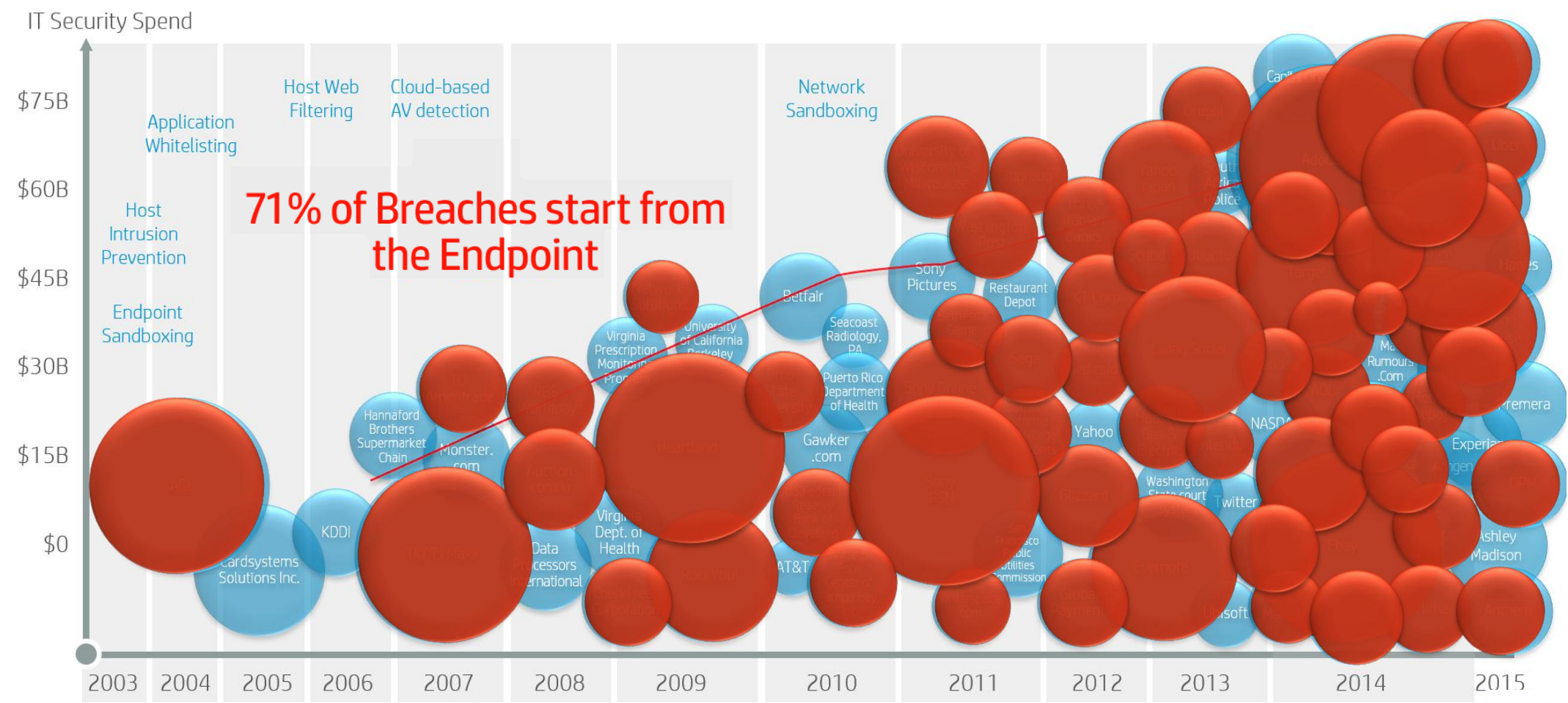
Exploit breakdown: No longer for “script kiddies” , or even organized crime

- Individuals used to hack for mischief and notoriety
- **THEN**, for profit
  - Identity theft
  - Ransomware
- **NOW**, for destruction and damage
  - State sponsored (Nation States)
  - Activists
  - Unlimited funding
  - Targets (Any & All):
    - ✓ Any Verticals, Supply Chain
    - ✓ SMB, Sub-Contractors,
    - ✓ Line Level Individuals





# The weakest link





# MORE

...

**DATA**  
40ZB  
By 2020

**CLIENTS**  
25B "Connected  
Things"  
By 2020

**SECURITY  
THREATS**  
+48% Annually





# Endpoint vulnerabilities



- Malware & viruses
- Device access
- Data flows between devices and network
- Data on hard disks
- Device configuration
- Visual hacking
- Physical loss or theft
- Fraud and counterfeit

[www.isaca.org/state-of-cybersecurity-2016](http://www.isaca.org/state-of-cybersecurity-2016)

[http://www.verizonenterprise.com/resources/reports/rp\\_data-breach-investigation-report\\_2015\\_en\\_xg.pdf](http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf)

<http://investors.3m.com/news/press-release-details/2016/New-Global-Study-Reveals-Majority-of-Visual-Hacking-Attempts-Are-Successful/default.aspx>



# HACKING UNSECURED PRINTERS IS EASY

I probe around for a multifunction printer and see that it is configured with default passwords. Great, I am in..."

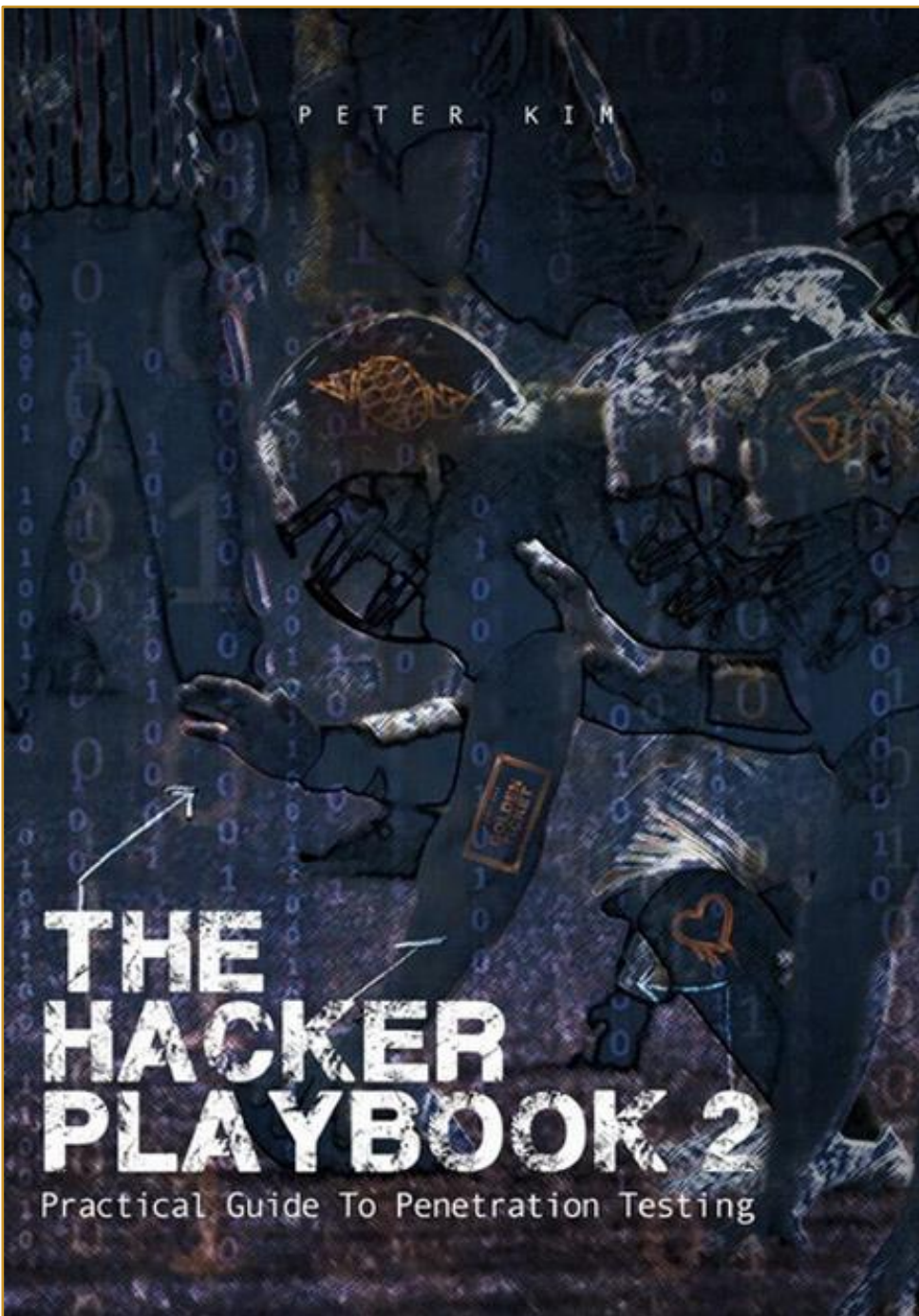
---

- PETER KIM

Industry-Leading  
Penetration Tester, Hacker,  
Author

---

We've compromised a number of companies /Organization using printers as our initial foothold. We move laterally from the printer, find Active Directory, query it with an account from the printer and bingo, we hit GOLD..."

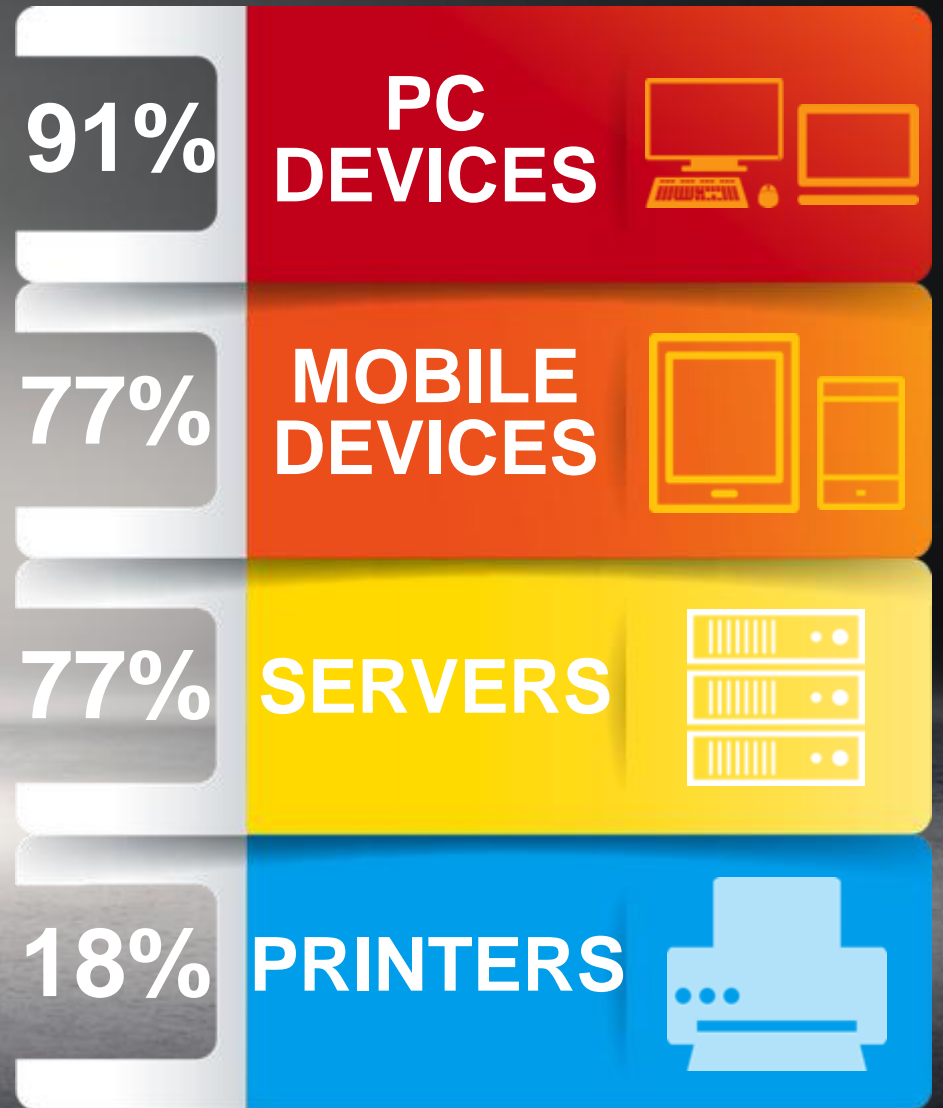




# AND YET, PRINTING IS NOT A HIGH SECURITY PRIORITY FOR MANY ORGANIZATION WORK



## LEVEL OF CONCERN



Source: Spiceworks survey of 107 IT pros at companies with 250 or more employees in North America, Europe, the Middle East, Africa, Asia Pacific, and China, conducted on behalf of HP in January 2015,



# HACKER THREATS

92%

REPORT DATA  
BREACHES

– Forbes Global 2000

65%

BREACHES ARE  
EMPLOYEE  
ERROR

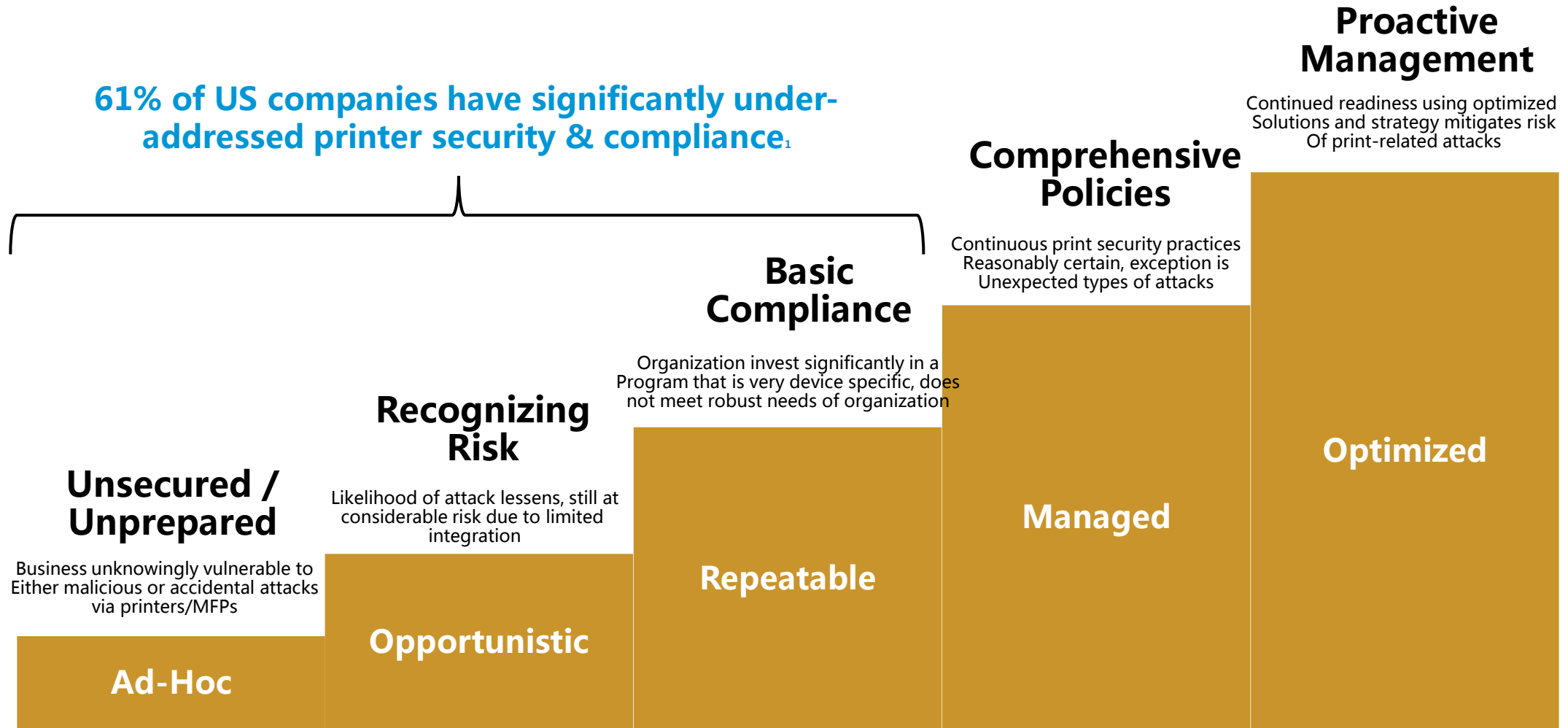
\$7.7M

AVERAGE COST OF  
A DATA BREACH



# Print Security Stages of Maturity ( 2016 March )

61% of US companies have significantly under-addressed printer security & compliance<sup>1</sup>



<sup>1</sup>IDC, "IDC MaturityScope Benchmark: Print Security in the United States," March 2016 IDC#US41048016  
<sup>2</sup>IDC, "IDC MaturityScope: Print Security", December 2015



# What is an End Point?





# A Brief History of Printer Hacks



## NEWS

MAR 25 2016, 4:06 PM ET

# Printers at 12 Colleges Spew Hate Fliers in Suspected Hack

by CORKY SIEMASZKO

Just days before Easter, anti-Semitism reared its ugly head again — this time in filth-filled fliers that suddenly showed up in campus printers at a dozen universities across the country.

"White Man are you sick and tired of The Jews," the hateful message begins on the single-page missive that is adorned with swastikas and includes the web address for a neo-Nazi group.

The fliers were found at universities ranging from DePaul University in Chicago to the University of Massachusetts in Amherst to UCLA out in Los Angeles, according to the [Anti-Defamation League](#) and various published reports.

"We don't know whether this was timed to Easter, or not," said the ADL's Todd Gutnick.

DePaul University said it suspects their printers [were hacked](#) are now taking steps to secure them from future breaches.

"We are currently investigating the breach as well as the source and origin of this despicable act, which certainly is not reflective of DePaul's values nor of our campus culture where all are welcome," said the Rev. Dennis Holtschneider, the university's president.

Holtschneider also urged students and campus workers to destroy the fliers if they find them.

advertisement



## FROM THE WEB

Sponsored Links



People are Moving from Retail to Online for Glasses - Here's Why!

[@ShopperUSA.com](#)DEPAUL  
UNIVERSITYPRINCETON  
UNIVERSITYSMITH  
COLLEGE

MOUNT HOLYOKE



BROWN

UMASS  
AMHERST



KIM ZETTER SECURITY 10.05.15 7:00 AM

# HACKING WIRELESS PRINTERS WITH PHONES ON DRONES



YOU MIGHT THINK that working on a secured floor in a 30-story office tower puts you out of reach of Wi-Fi hackers out to steal your confidential documents.

But researchers in Singapore have demonstrated how attackers using a drone plus a mobile phone could easily intercept documents sent to a seemingly inaccessible Wi-Fi printer. The method they devised is actually intended to help organizations determine cheaply and easily if they have vulnerable open Wi-Fi devices that can be accessed from the sky. But the same technique could also be used by corporate spies bent on economic espionage.

SHARE



SHARE 835



TWEET



PIN



COMMENT 5



EMAIL



## LATEST NEWS



DIVERSITY  
Etsy Is Defying Tech's Lousy Record on Gender Diversity  
15 HOURS



BUSINESS  
Whoa, Amazon Isn't Just Making Money. It's Making More Than Ever  
15 HOURS



UNRELATED  
A Brief History of the Internet  
15 HOURS

# WIRELESS HACKING

Researchers in Singapore developed a drone with a mobile phone that can detect open wireless printers in close proximity then establish the mobile device as a fake access point that mimics the printer and intercepts documents intended for the real device.

**iTrust**  
Center for Research in  
Cyber Security





## Hacker came in via label printer: Train Danish company's IT systems hostage

Hacker sneaked in through a label printer attached to a Windows XP machine with Danish color wholesaler. All company data was encrypted and only released on payment of ransom. The company took first money out. But then switched opinion and took up the fight.

April 17, 2015 at 16:12





# Customer Photo – Network Sniffing.

Cupboard →





HACKERS CAN HEAR ALL BY ....





# HP PC and Printing security leadership



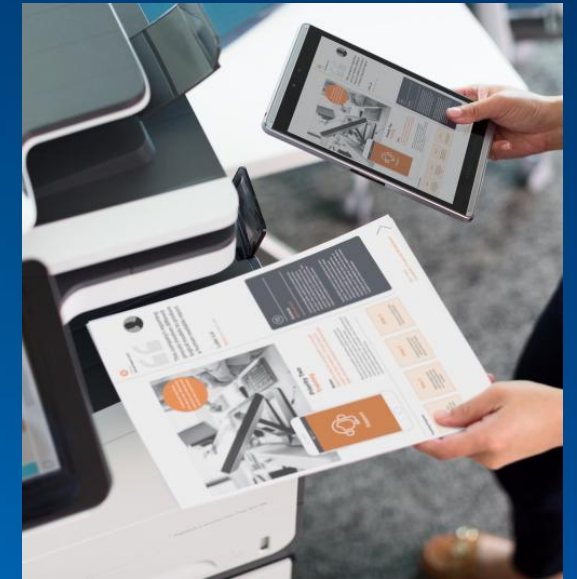
Device



Identity



Data



Documents



# Today's printers look a whole lot like PCs

Yet only 53% of IT managers realize printers are vulnerable to cyber crime<sup>1</sup>



Today's printer is a fully functioning client on a network



Hardware



Firmware and software



Internet



Email



Network access

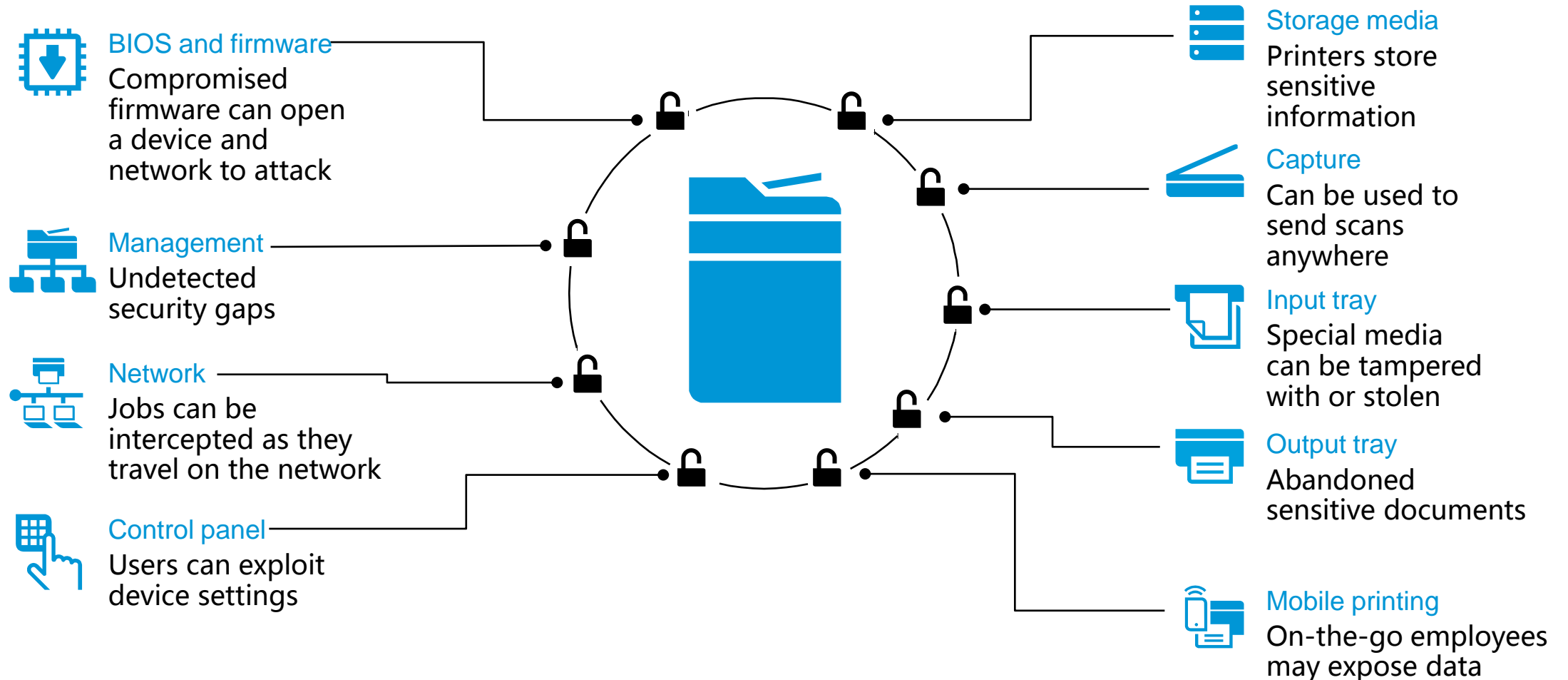


<sup>1</sup>Ponemon Institute, "Annual Global IT Security Benchmark Tracking Study", March 2016.



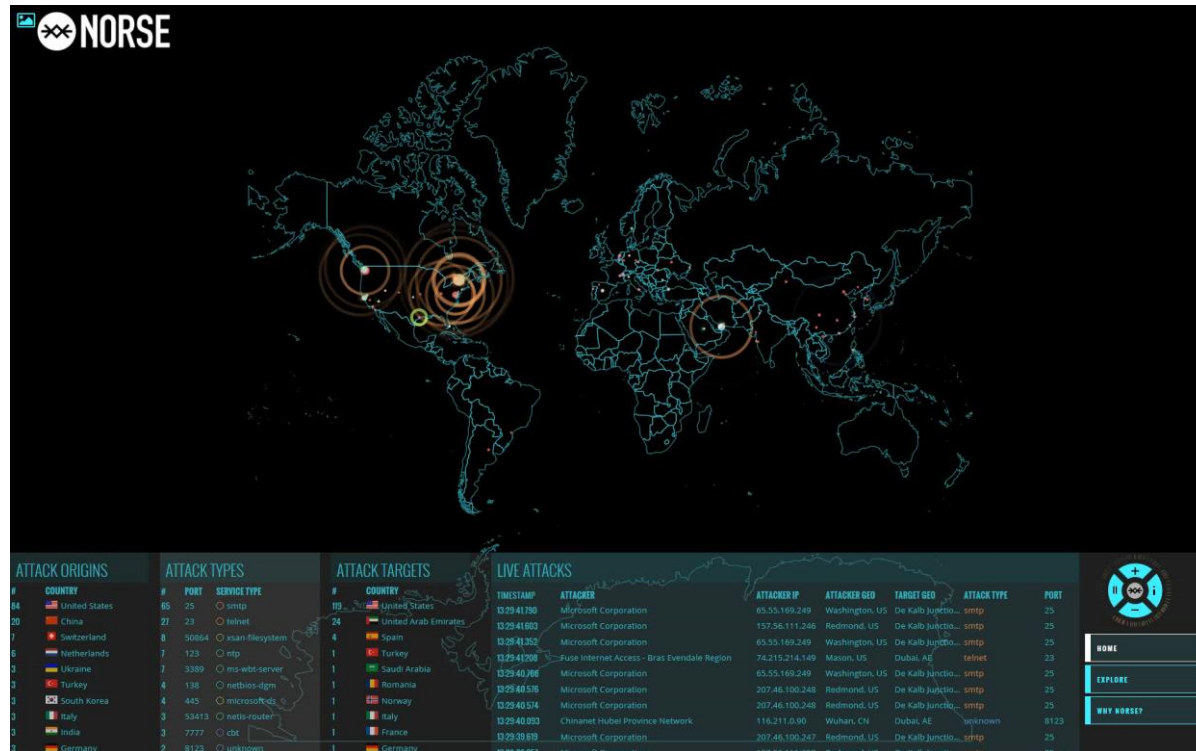
# The Basics — printing carries risk

Vulnerabilities across device, data and document need to be managed





# Attacks are Global and happening every second



<http://map.norsecorp.com/>



<https://cybermap.kaspersky.com/#>



# HP state-of-the-art device security



- Built-in threat detection and remediation
- **HP Sure Start**
  - Industry's only self-healing BIOS
- **Whitelisting**
  - Guaranteeing only the right firmware runs on the device
- **Internal runtime intrusion detection**
  - Industry's only self-monitoring capability



# Document and physical security

Confidential document controls, visual hacking preventions & locks



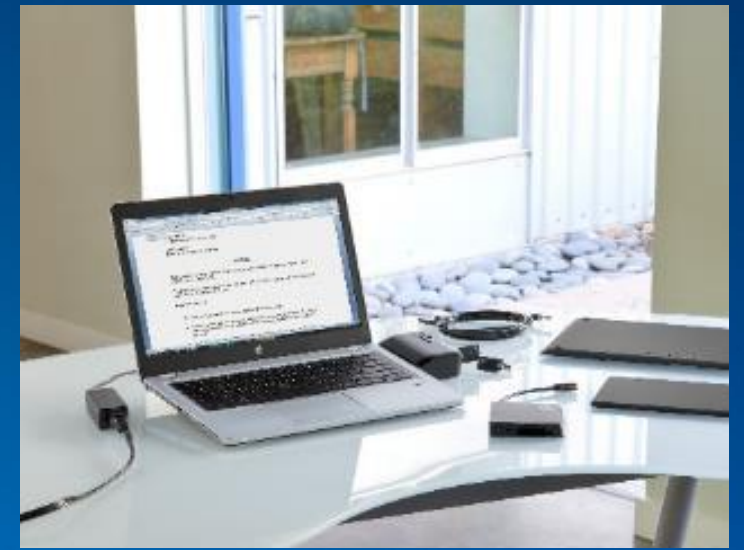
## Control access

Add pull print software & card readers to meet compliance and lower printing costs with minimal user impact



## Visual hacking prevention

The world's only integrated privacy screen, HP Sure View. Simple to use and protection starts at 35% from center.



## Physical theft prevention

HP has a broad range of security accessories



# Layers of security defenses

## HP Secure MPS approach

Comprehensive security comes from layering the industry's strongest security defenses.

1. Security best practices start with secure devices and device management services to harden devices and secure network connections
2. Next add additional security layers based on a custom risk assessment and security plan
3. Then overtime, maintain and evolve security efforts relative to the evolving threat landscape



### Secure printers & MFPs

- Built-in malware protection
- Encrypted hard drives

### Device hardening

- Admin passwords
- Firmware updates
- Configuration of interfaces & services

### Monitor for threats

- Vulnerability assessments
- SIEM integration

### Data encryption & user authentication to the device

### Data and Document confidentiality

- Advanced authentication & control of access
- Process and workflow changes
- Anti-fraud, anti-counterfeit solutions



# HP Security Solutions



1. Output tray
2. Hard disk
3. Network card
4. Control panel
5. Secure input tray
6. Printing fleet





# HP Helping Vertical Below on Securing This Documents

HP SOLUTION TO GOVERNMENT, FINANCE, LEGAL, CORPORATION, EDUCATION

- **A large number of companies rely solely on preprinted security paper** to protect their **high value documents**. Though preprinted security paper does a good job of **securing the base document**, it does not address the **security of personal data** that is added to the **document at the point of print**.
- By not **securing personal data**, companies are leaving themselves vulnerable to **unauthorized modifications, forgery or photocopying**. HP helps companies by adding another **layer of protection to their documents**. By adding **personalized security features to each print file** before it is **routed to the printer**, companies can now add in a layer of security beyond preprinted stock, helping to **create unique and secure documents**.
- **Government**
  - Birth Certificates, Death Certificates, Marriage Licenses, Vehicle & Equipment Registrations, Real Estate Titles and Deeds, Work Visas, Temporary IDs, Driver' s Licenses, Passports, Resident/Work Permits, Government IDs
- **Education**
  - Transcripts, Grade Reports, Certifications, Degrees, Diplomas
- **Legal**
  - Contracts, Wills, Power of Attorney Documents Certificates
  - of Origin, NDAs, Background Checks, Client Records





# Risk: Unauthorized copies

## Solution: HP Copy Protection solutions

### Copy-Void

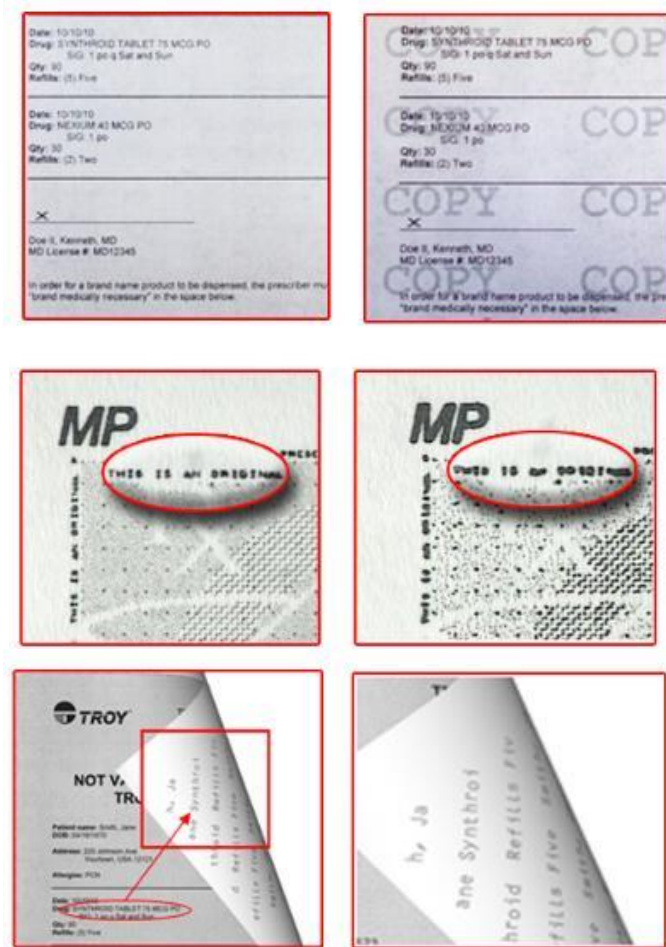
A hidden COPY message, printed behind document information, is revealed by **unauthorized copying**.

### Micro Printing

Customizable microprint indicates a copy under magnification.

### TROY Mark

A repeating “watermark” of user defined variable document data across the front or back of each document.





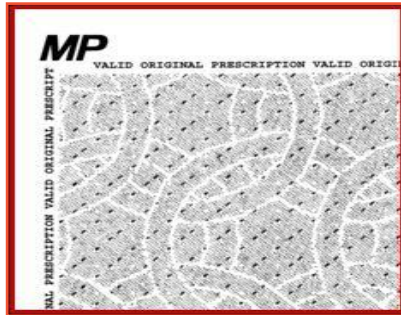
# Tamper proof university certificates



## Layered approach to document security

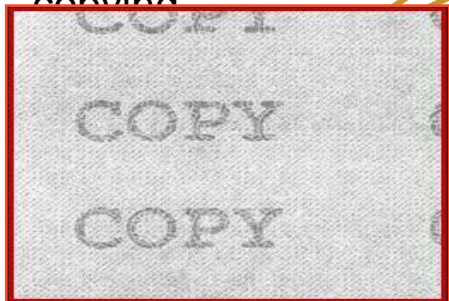
### Microprinting

Customizable  
TROY microprint  
indicates a copy  
under magnification



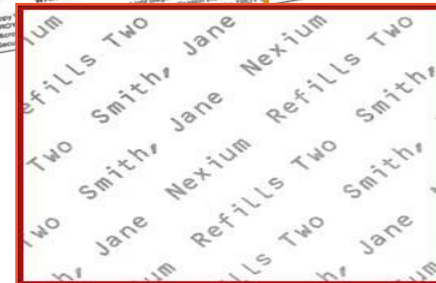
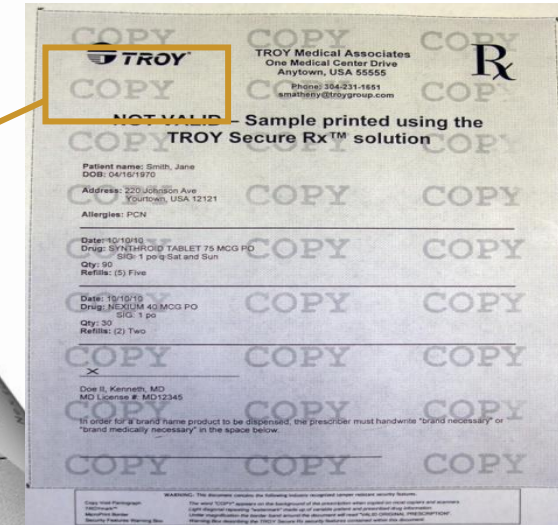
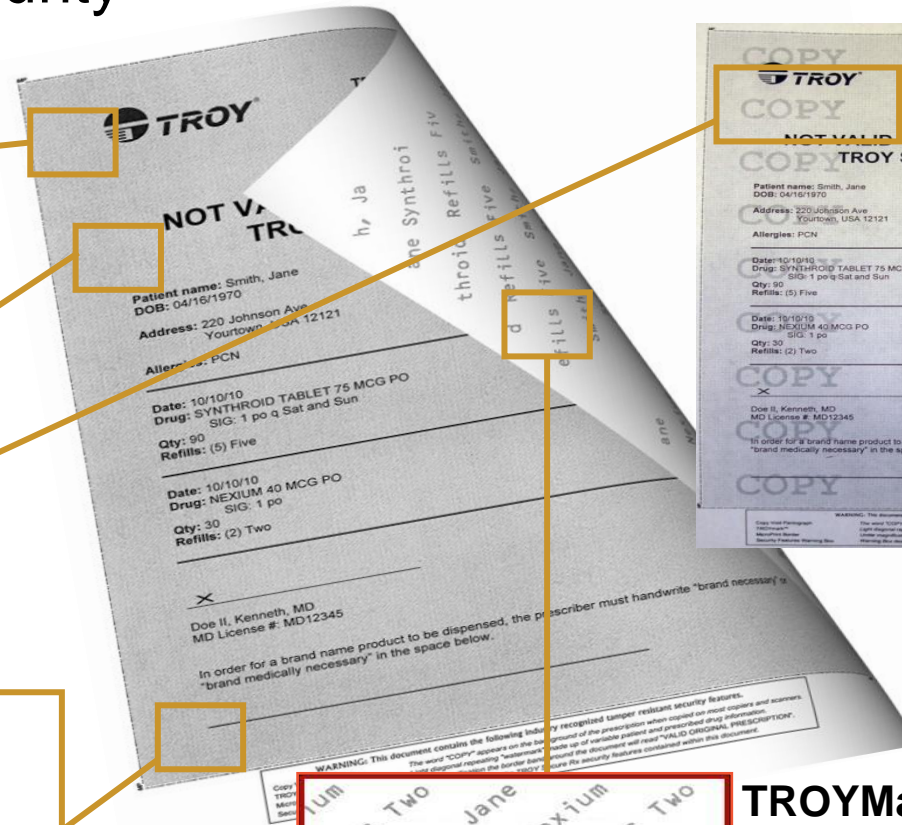
### TROY Copy-Void

A hidden “COPY”  
message printed behind  
document is revealed  
by unauthorized  
copying



### Plain paper

TROY SecureRx uses  
plain paper: No  
expensive pre-printed  
stock to purchase,  
inventory, and secure  
from theft.



### TROYMark™

TROY SecureRx prints a  
repeating watermark of  
user defined variable data  
across the back of each  
document.





# Creating

# the future together

