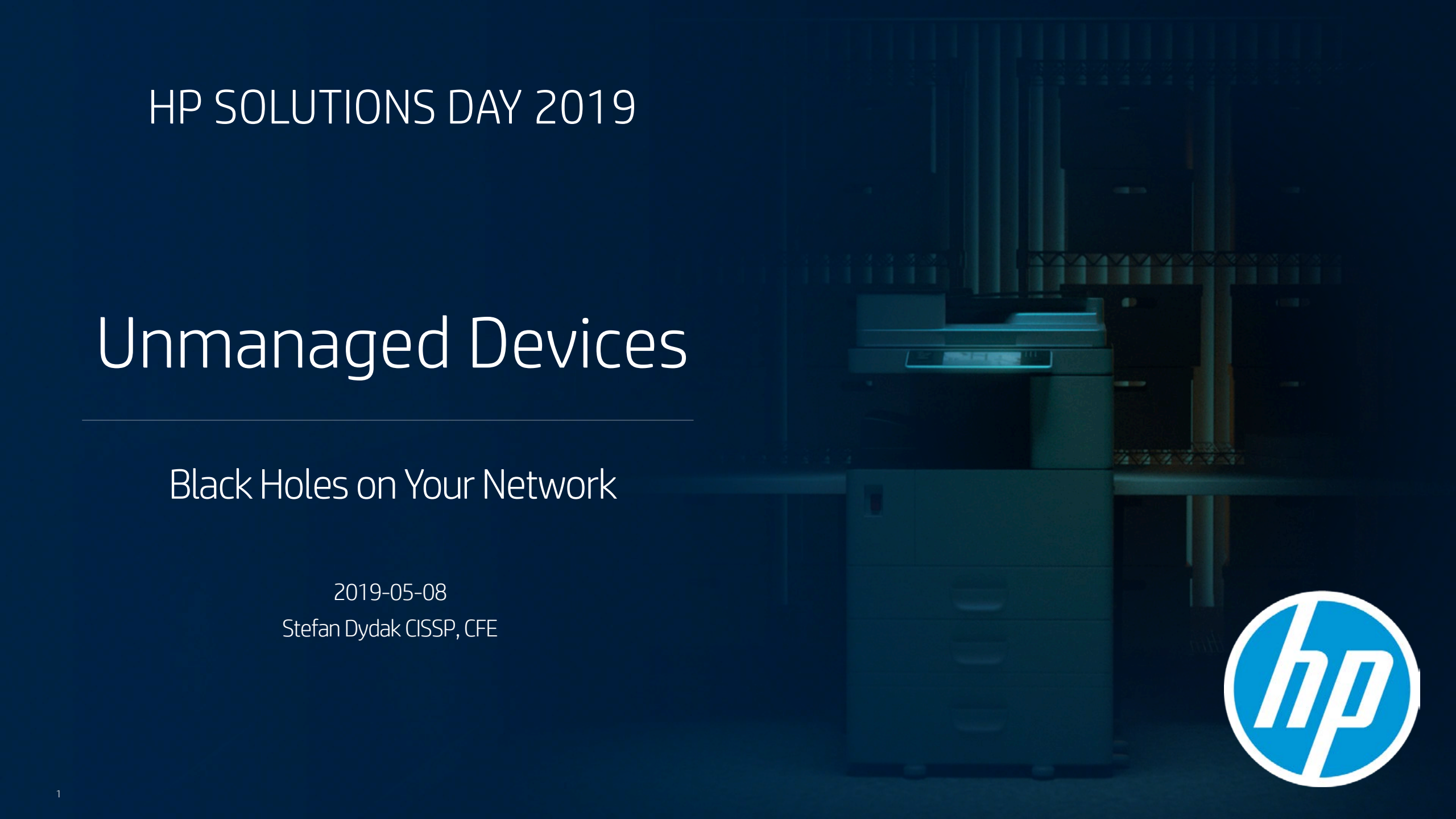
HP SOLUTIONS DAY 2019

Unmanaged Devices

Black Holes on Your Network

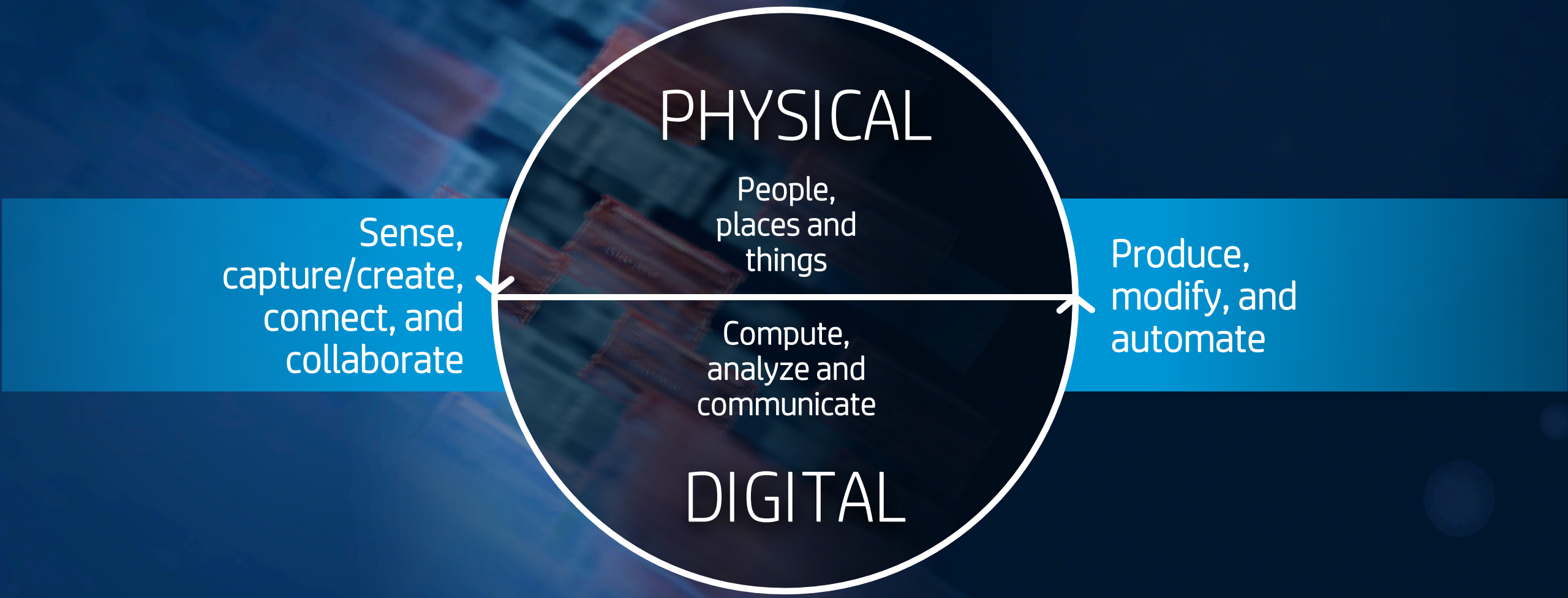
2019-05-08

Stefan Dydak CISSP, CFE

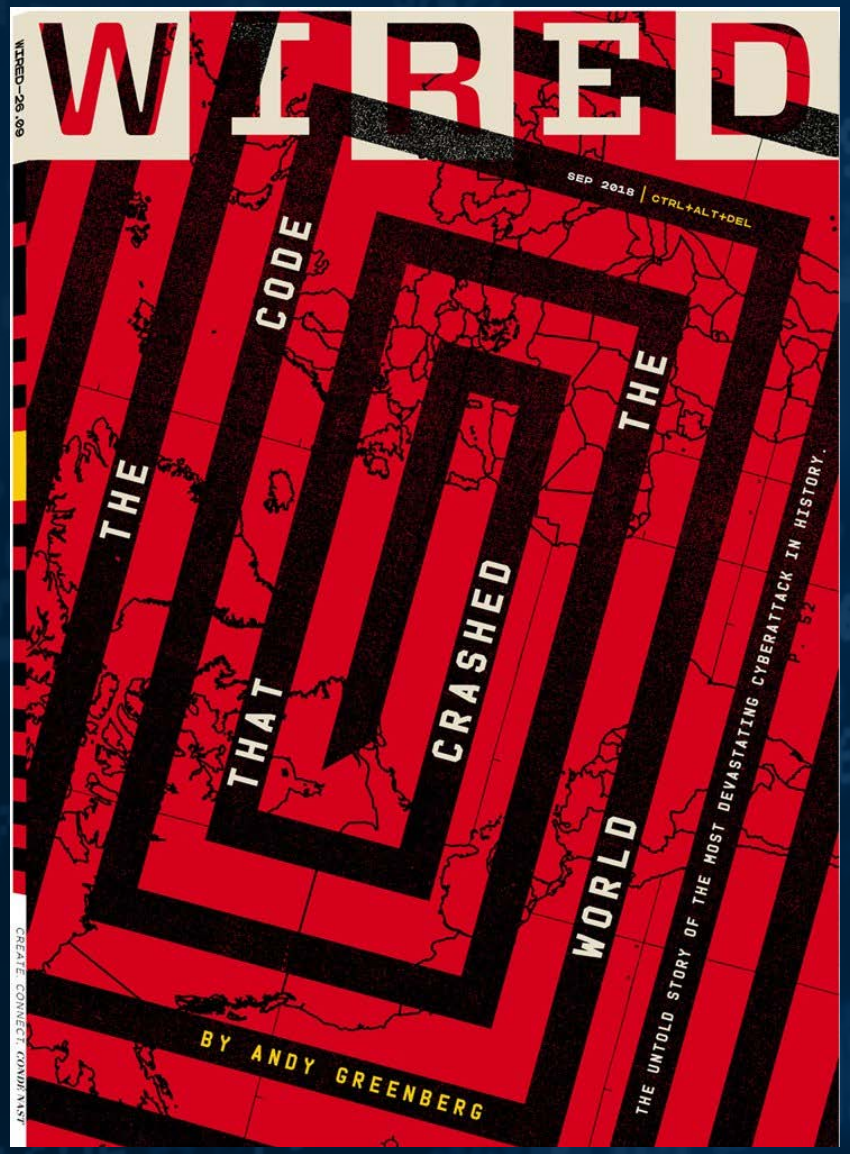


The Internet of Vulnerabilities

When Worlds Collide



Digital Risks become Physical

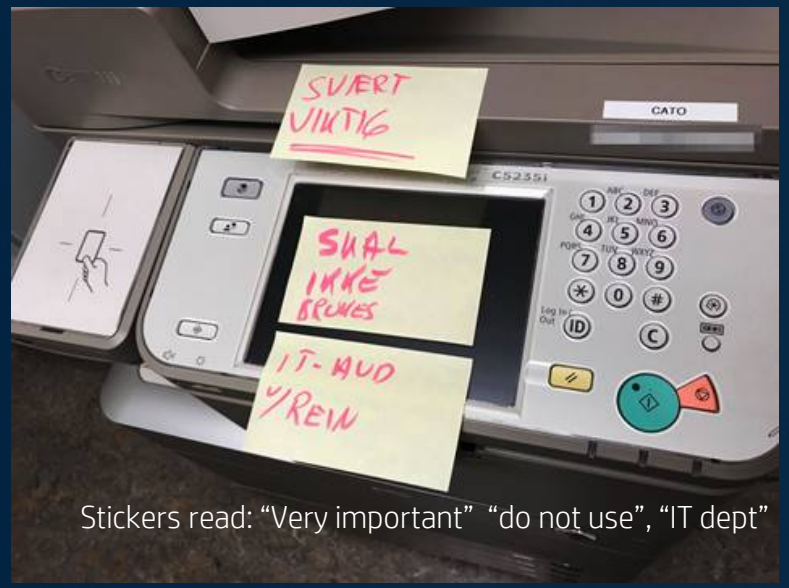


Three reasons for avoiding the endpoint security decision

"I see Endpoints as commodities"

"My Next Generation endpoint protection Suite adequately monitors all my endpoints"

"Printers – what's the worst that can happen?"



Stickers read: “Very important” “do not use”, “IT dept”

September 2018

Norwegian Parliament shut down several MFPs due to security concerns and investigation following possible foreign intelligence/espionage situation.

Printernekt på Stortinget etter spionpågripelsen på fredag

Det står skrevet store advarsler på printerne i deler av Stortingsbygget, etter at en nå spionsiktet russer deltok på seminar der.

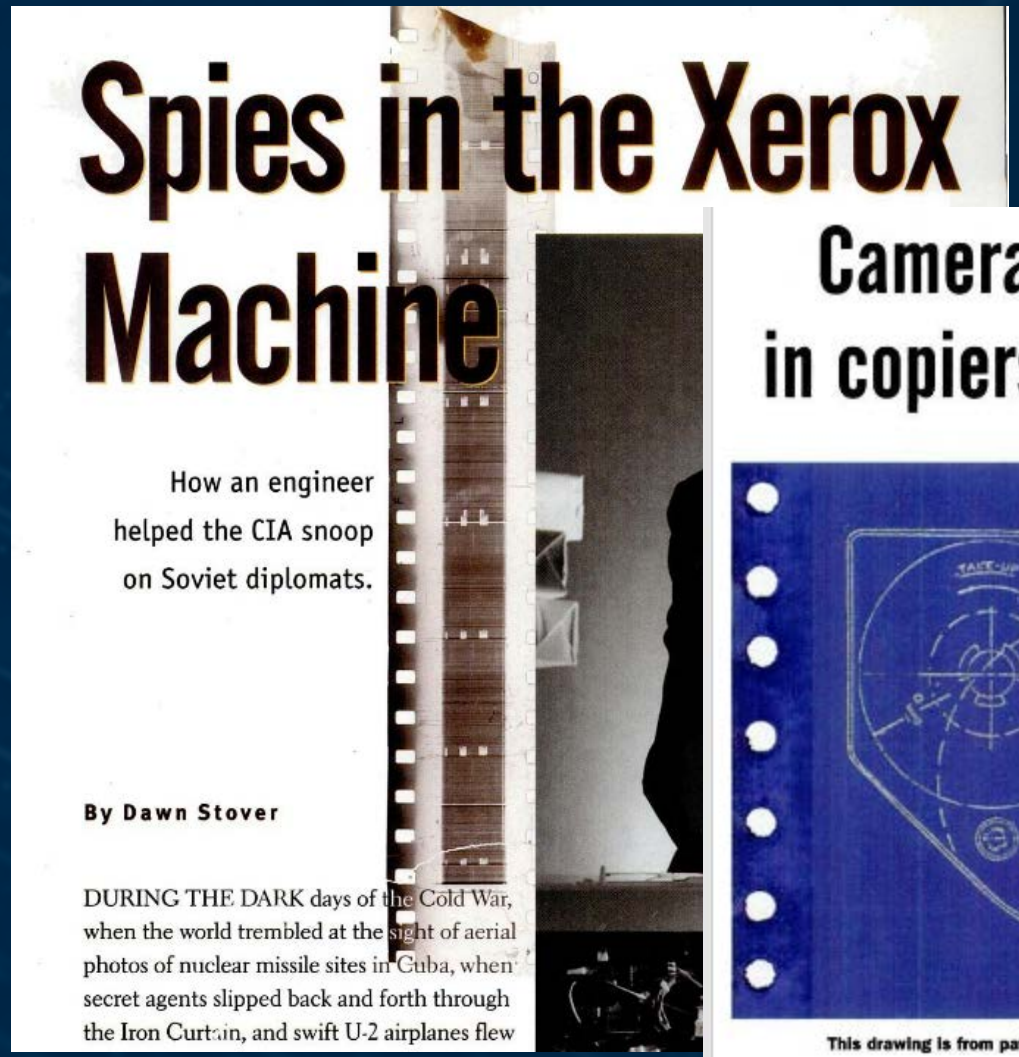
WORLD NEWS SEPTEMBER 24, 2018 / 8:31 AM / UPDATED 21 HOURS AGO

Moscow protests Russian's arrest in Oslo, Norwegians seal off room in parliament

Nerijus Adomaitis, Maria Tsvetkova 4 MIN READ

OSLO/MOSCOW (Reuters) - Russia’s foreign ministry summoned Norway’s ambassador on Monday to protest against the arrest of a Russian citizen in Oslo on suspicion of spying while Norwegian authorities sealed off what was described as a “compromised room” in parliament.

First “Printer” Hack … 1963



Spies in the Xerox Machine

How an engineer helped the CIA snoop on Soviet diplomats.

By Dawn Stover

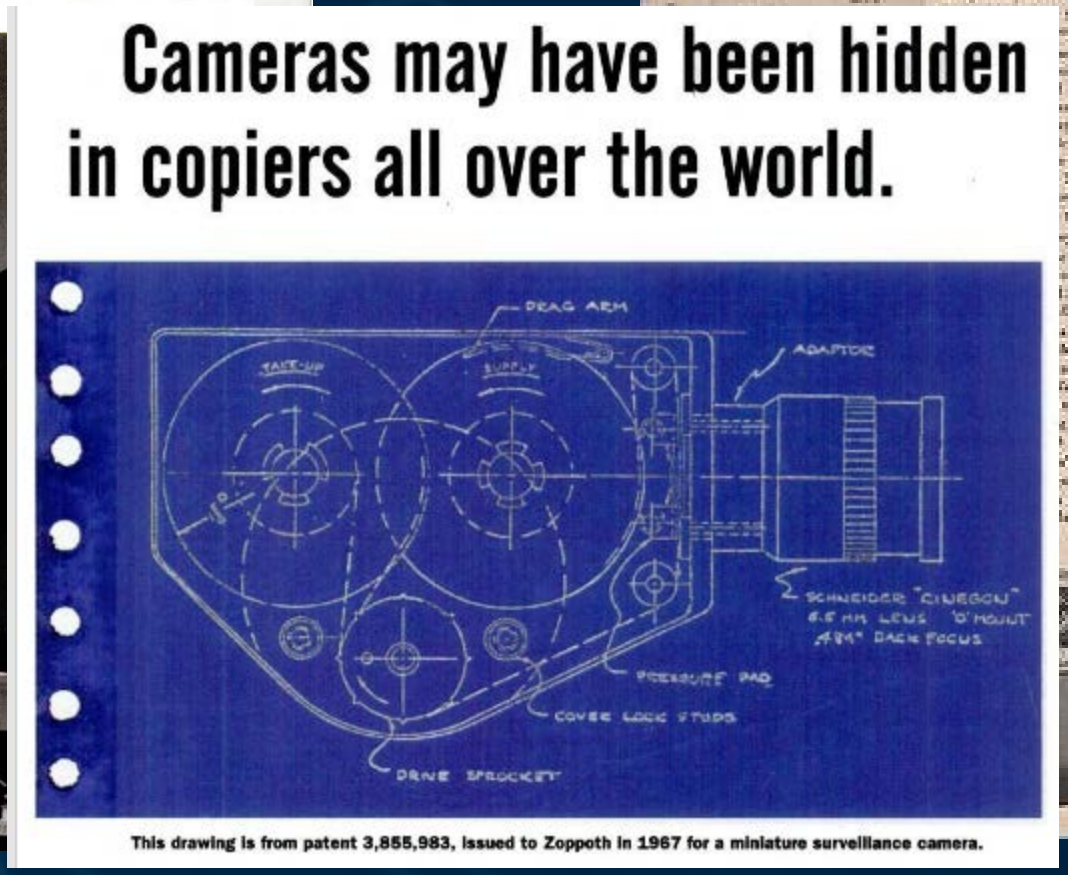
DURING THE DARK days of the Cold War, when the world trembled at the sight of aerial photos of nuclear missile sites in Cuba, when secret agents slipped back and forth through the Iron Curtain, and swift U-2 airplanes flew

Xerox 813 Special. Here's what you get for $1.08 a day.

How much does copying paper cost?

Where can you see the 813?

XEROX

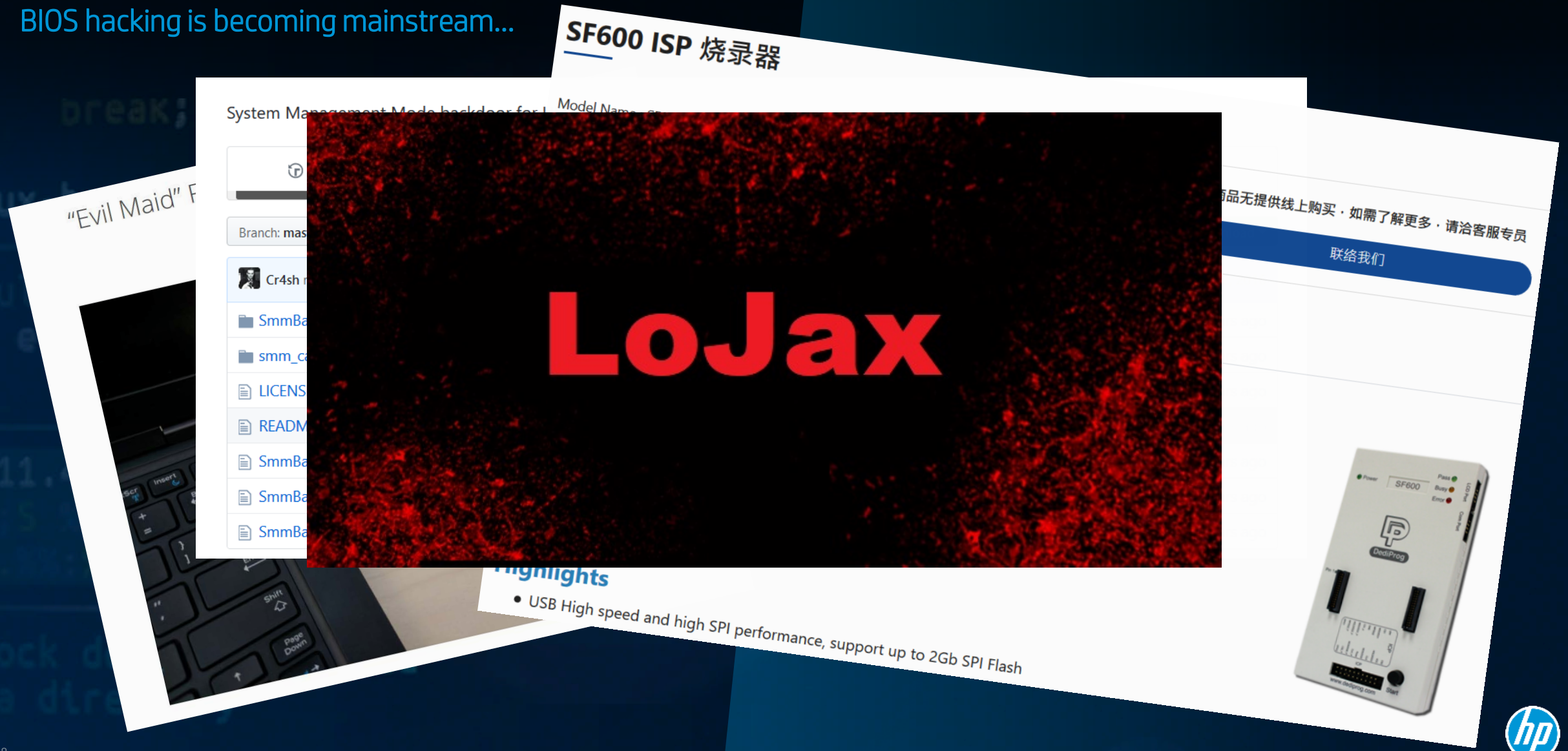


Cameras may have been hidden in copiers all over the world.

This drawing is from patent 3,855,983, issued to Zoppoth in 1967 for a miniature surveillance camera.

PC Firmware Hack for all

BIOS hacking is becoming mainstream…



ENDPOINTS ARE THE FIRST POINT OF ENTRY

Enterprise data center and cloud services

SECURITY

ANTICIPATING THREATS

- Future devices will need to survive future threats
- Analyzing emerging threats and attack trends to inform security research
- Analyzing and detonating malware state of-the-art in our own Malware Lab

DESIGN FOR CYBER-RESILIENCE

SECURITY BUILT-IN FROM THE HARDWARE UP

Software / network security are not enough

Must start from the hardware up

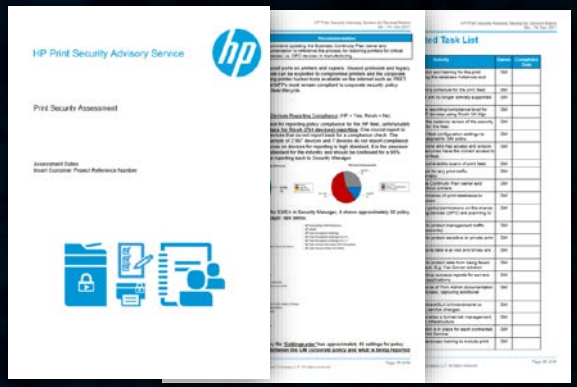
But Security is not only about Technology....

HP Security Advisory Service

Onsite risk assessment

Identify the Risk & Estimate impact

Provide recommendations (security roadmap)

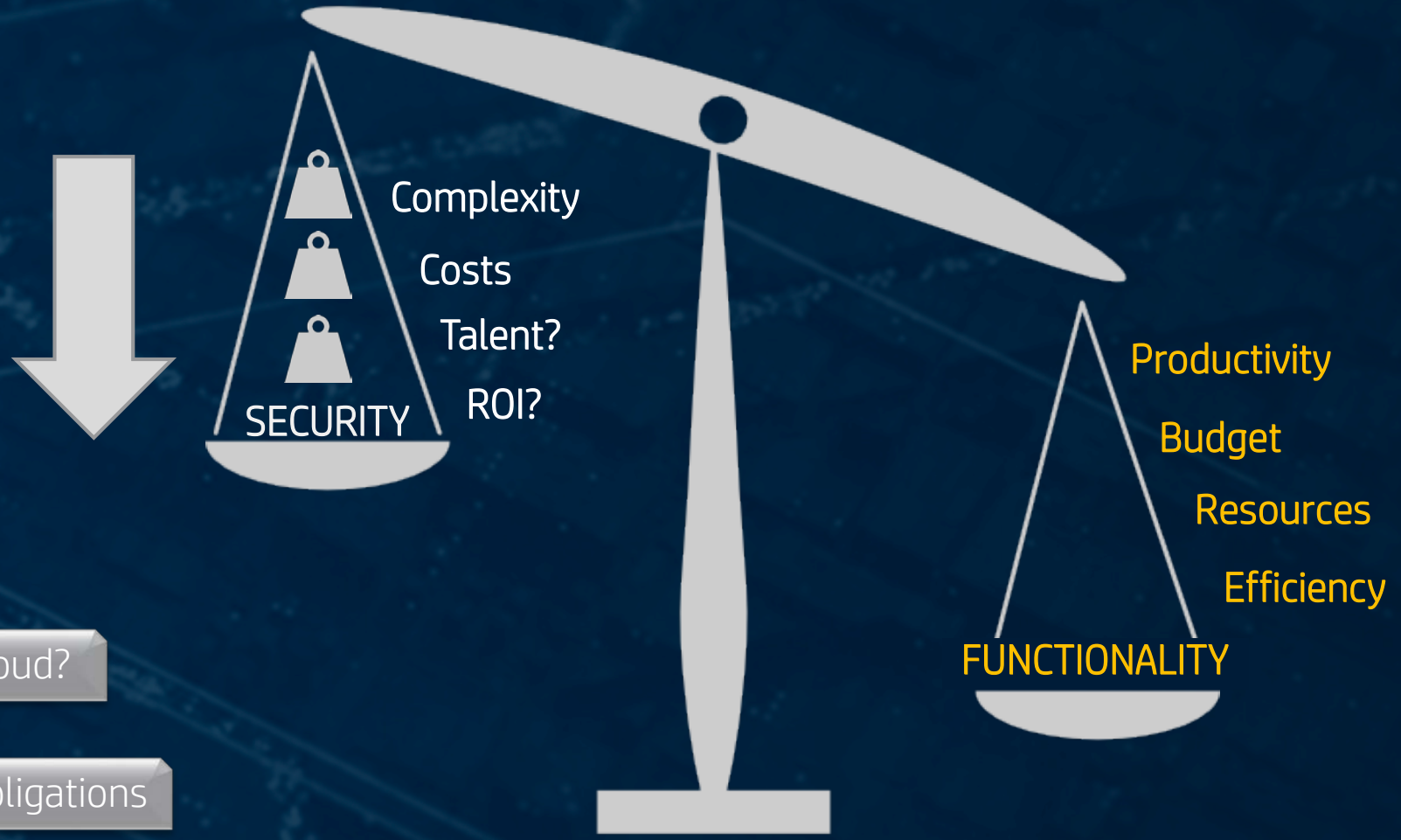


Unknown Risks

Identify & Mitigate

Manage residual risk

The Classic Trade-Off



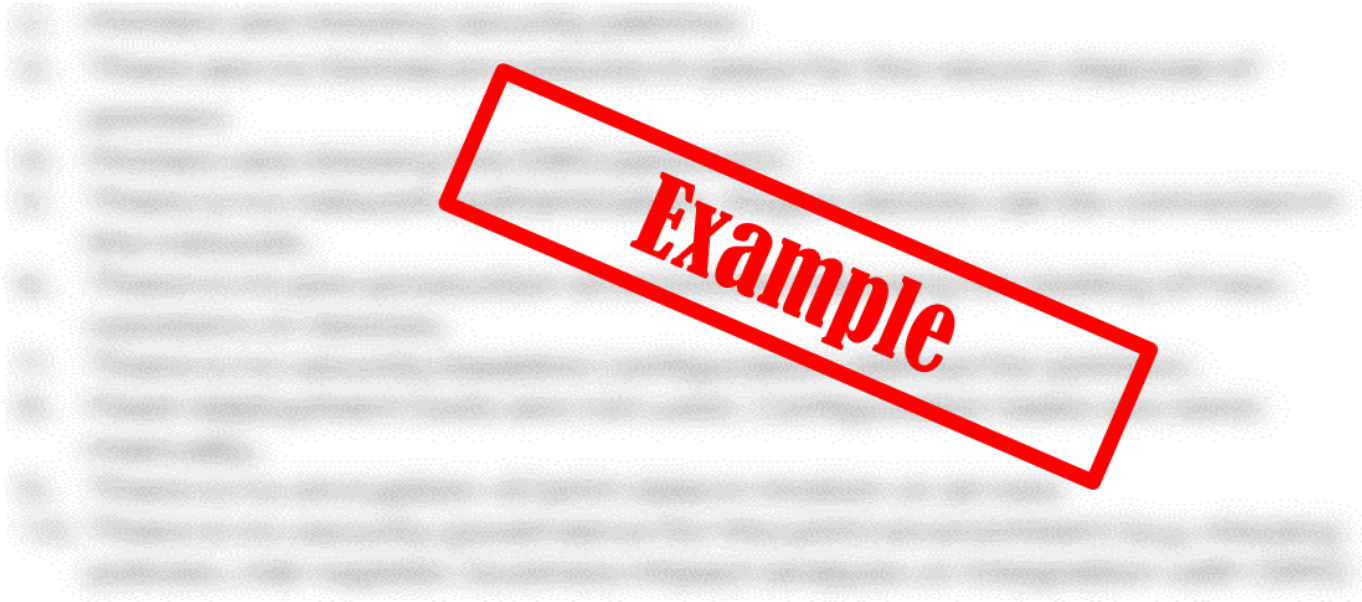
- Move to the Cloud?
- Contractual Obligations
- Cybercrime and Compliance

SAS Results – Ugly Truths

- Misalignment between Governance and Operations
- Asset Management & Configuration
- Patch Management
- LifeCycle Management & Business Continuity
- Data Security
- Logging and Monitoring Activities

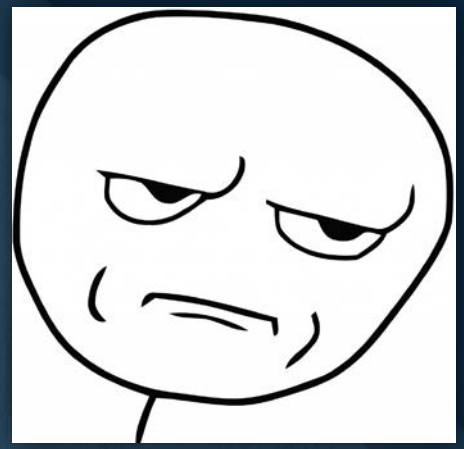
Top Findings

1. The printing environment is divided in a well-managed, centralised, environment (e.g. MFPs) and a decentralized, unmanaged environment (e.g. label printers, plotters). These unmanaged devices were found to be missing even the most basic security hygiene.
2. The whole printing environment is proactively managed, but there is no detective or reactive security component in place. Configuration or log event monitoring is non-existent and any security incidents originating from print solutions or devices may go unnoticed.



Security by Obscurity

“If no one notices the endpoint is vulnerable, then it isn’t vulnerable”

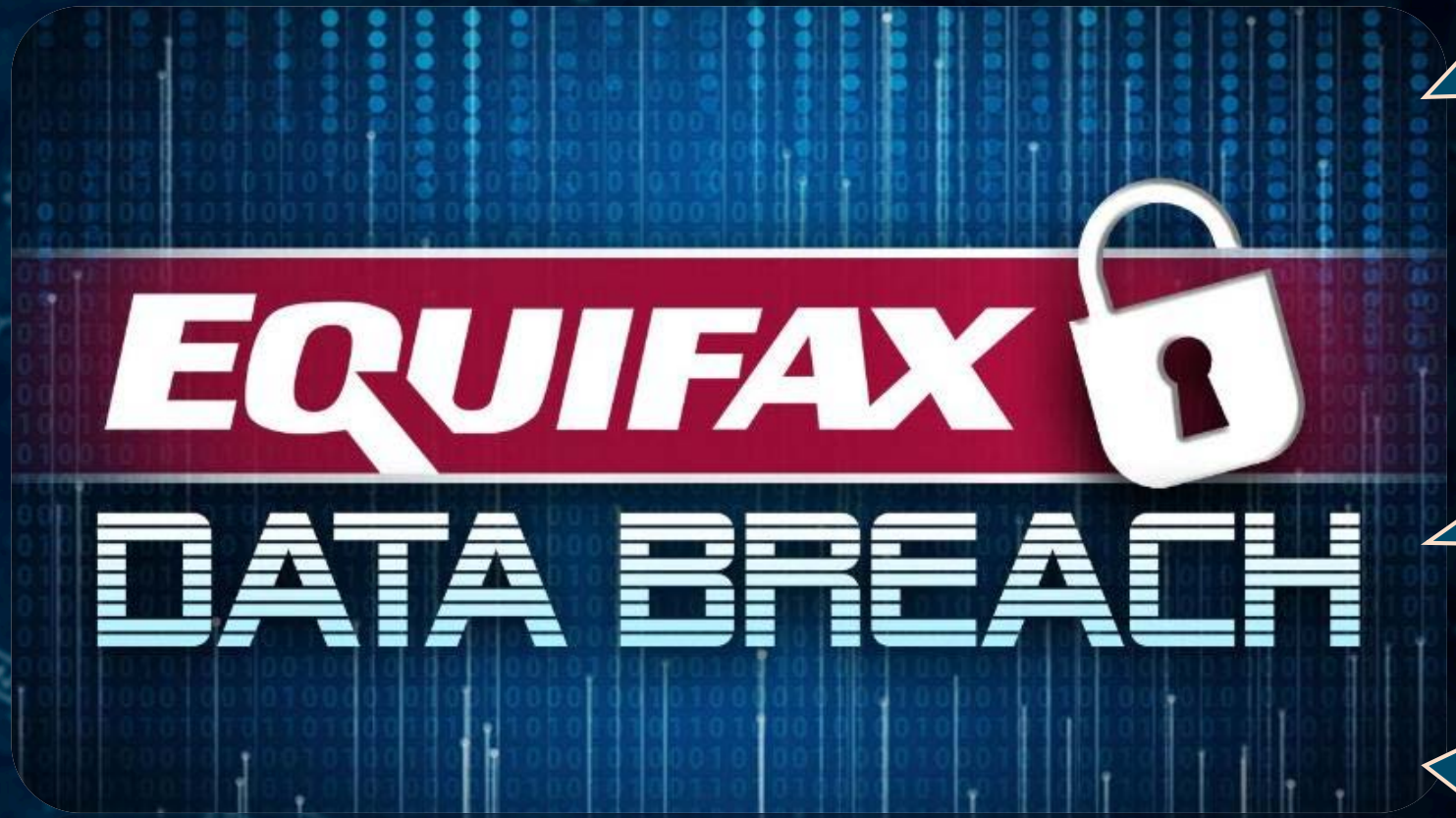


Where have we seen all this before?

Legacy System compromised (1970!)

Inaccurate list of Assets

Disconnection between ITSEC and Operations



Access Control not implemented correctly (DB access not restricted or monitored)

PII data, Usernames and Passwords stored in un-encrypted files

Network Segmentation missing for the compromised Apps. (DMZ access to parts of the network)

Security Standards & Guidelines not enforced

IDS/IDS had expired SSL certificates

Upon update, immediate detection of suspicious traffic

End to End Security

Security Services

Security assessments, security implementation, ongoing compliance, risk management

Management and monitoring solutions

End-to-end security and monitoring solutions (data, devices, documents…)

State of the art secure devices

Protection, detection and recovery capabilities at the deepest level

Thank You
Stefan Dydak
EMEA Senior Security Advisor