LET'S CONNECT

PRINECT
USER DAYS

Security in the Print Shop:

Successfully fending off Cyber Threats

Disclaimer

Legal notice

The contents of this workshop have been prepared with the greatest care. The workshop and the information provided therein are in no way a substitute for experts, individual advice from knowledgeable third parties. Heidelberg accepts no responsibility for correctness, completeness, and accuracy of the information provided.

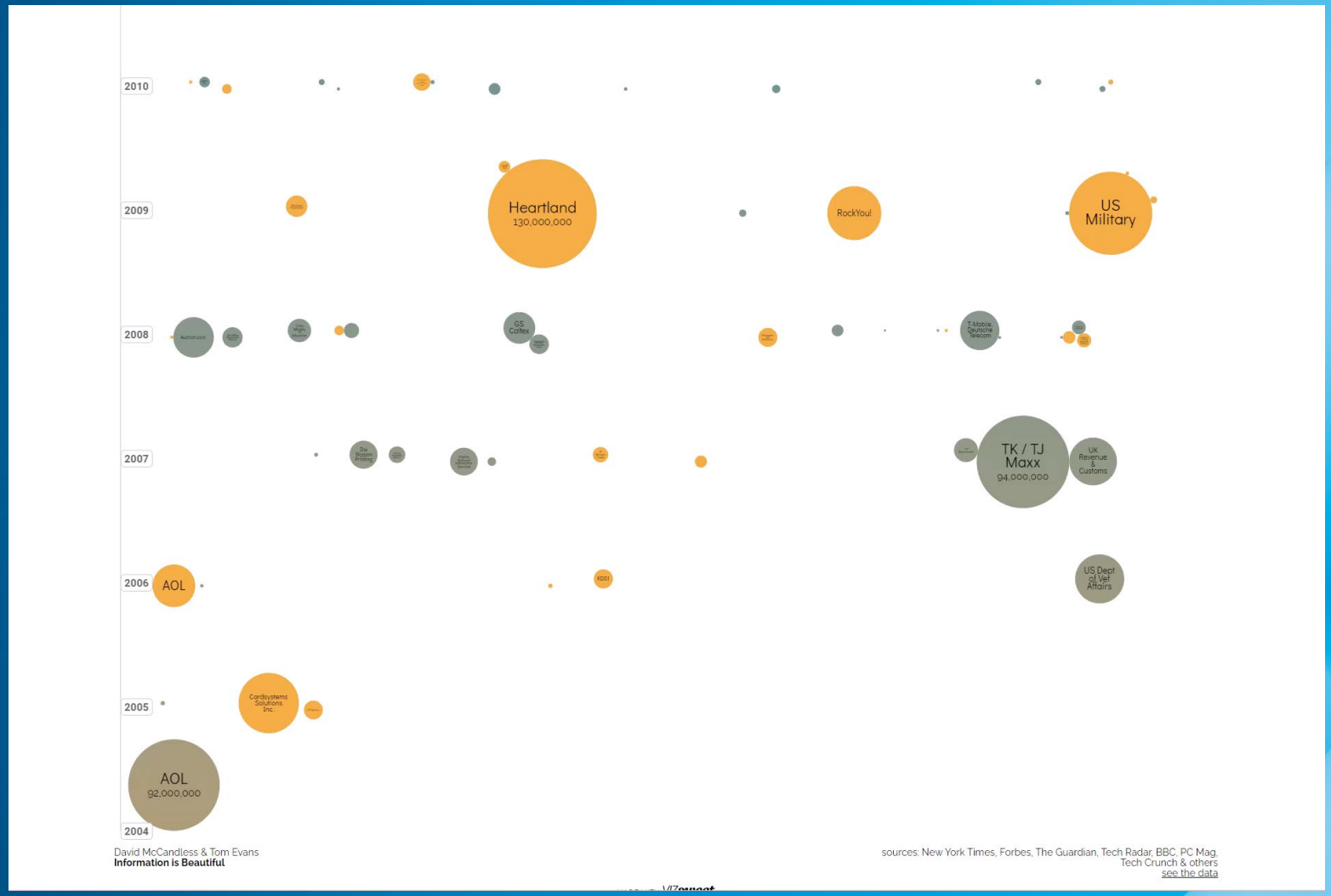
Threat Scenarios

The Biggest Attack Trends

AI-based attack methods	▪ Deepfakes ▪ Voice Cloning
Phishing and social engineering	▪ Spying on sensitive data of victims
Ransomware	▪ Blackmail after data encryption
Data theft	▪ Ransom or publication of your data
Cyber crime as a service	▪ The criminal as a customer of the hack industry ▪ Standardized, purchasable business models on the dark web
Supply chain attacks	▪ Infiltration of malware ▪ Are your partners well positioned in terms of information security?
Direct hack attacks	▪ The individual hacker attack
DDoS attacks	▪ System overload and paralysis ▪ Your business is blocked

World's Biggest Data Breaches & Hacks

Source: informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



Conclusion:

"It's not a question of if you will be hacked,
but when and how you respond."

Mark Minasi

How do you achieve a good security level?

1. Attitude thing → View security as a competitive advantage rather than an unnecessary cost

2. Adversary → Technical complexity and the human factor

3. Become active → Involve experts, implement and live best practices

Issues:

- What is necessary for a good level of security?
- How can I effectively protect my print shop against attacks?
- How secure are HEIDELBERG products and services?

A Good Own Protection Level

What is necessary for a good level of security?

Information Security Protection Goal:

Ensure
confidentiality, **integrity** and **availability**
of information

Identification of the most important assets and information and their protection needs

+

Analysis and evaluation of vulnerabilities and white spots on the security map

⇨ **Risk assessment**

How do you achieve a good level of security on your own?

Appointment of a security officer ***[****Chief (Information) Security Officer (CSO/CISO)]*

- is the driving force behind security in the print shop
- involved in decision-making processes
- responsible for Incident Response Team (IRT)

Information security is an ongoing process!

- requires continuous improvement
- perform security checks on a regular basis
- keep an eye on current threats and security trends
- maintain and continuously improve the level of protection

Effective Protection Against Attacks

How can I effectively protect my print shop against attacks?

Preventive Controls

Training and awareness:

- Train employees to deal with security risks and raise awareness of the threats caused by cyber attacks
  - Understanding information security
  - Ensuring data security as well as data protection
  - Ensuring physical security
  - "Best Practices" for secure computing, including remote and mobile working
  - What to do if there is a threat or violation?
- Detect phishing attacks, social engineering tactics, malware, data protection incidents
- Secure handling of (print) job data from customers/third parties

Access control:

- Limit access to sensitive data and systems to authorized users only
- Strong passwords, multi factor authentication (MFA), domain directory service

Software update and patch management:

- Keep all systems and software up to date
- Regularly install security updates and patches to address known vulnerabilities

How can I effectively protect my print shop against attacks?

Preventive Controls

Network security:

- Protect network from unauthorized access
- Implement security policies to monitor and filter traffic
- Secure web server (WAF, DMZ, reverse proxy, etc.)

Physical security:

- Protect physical access to critical resources such as presses, server room and sensitive documents

Firewalls and antivirus software:

- Deploy firewalls and antivirus software
- Monitor network traffic
- Detect harmful activities

(Print) data receipt/exchange:

- Check PDFs for malicious code (e.g. Adobe “protected mode”, opening customer data in “sandbox” environment, etc.)
- insecure FTP, SMB etc.: eliminate file sharing solutions

How can I effectively protect my print shop against attacks?

Detective Controls

Security Monitoring:

- Implement monitoring and analysis of network traffic to detect suspicious activity
- Intrusion Detection Systems (IDS): detection of unauthorized access
- Security policies and procedures: Establish policies and procedures to detect and respond security incidents

Corrective Controls

Incident Response Plan:

- Develop Plan to respond to security incidents
- Including detection, response and recovery from a cyber attack

Restorative Controls

Data backup and recovery:

- Create regular backups of data and systems that require protection
- Keep backups in a safe place
- Practice recovery (disaster recovery) regularly

How can I effectively protect my print shop against attacks?

Deterrent Controls

Network security:

- Network segmentation (office network, pressroom network...) to limit risks due to network isolation

Organizational Controls

Compliance and data protection:

- Ensure compliance with all relevant legal requirements and data protection regulations,
- especially if this concerns sensitive customer information
- Compliance with standards (such as payment standards)

Security policies and procedures:

- Develop and implement internal policies and procedures to ensure information security

Security of HEIDELBERG Products and Services

Shared Responsibility Model

ISMS certified according to ISO/IEC 27001

Shared Responsibility Model

Print shop

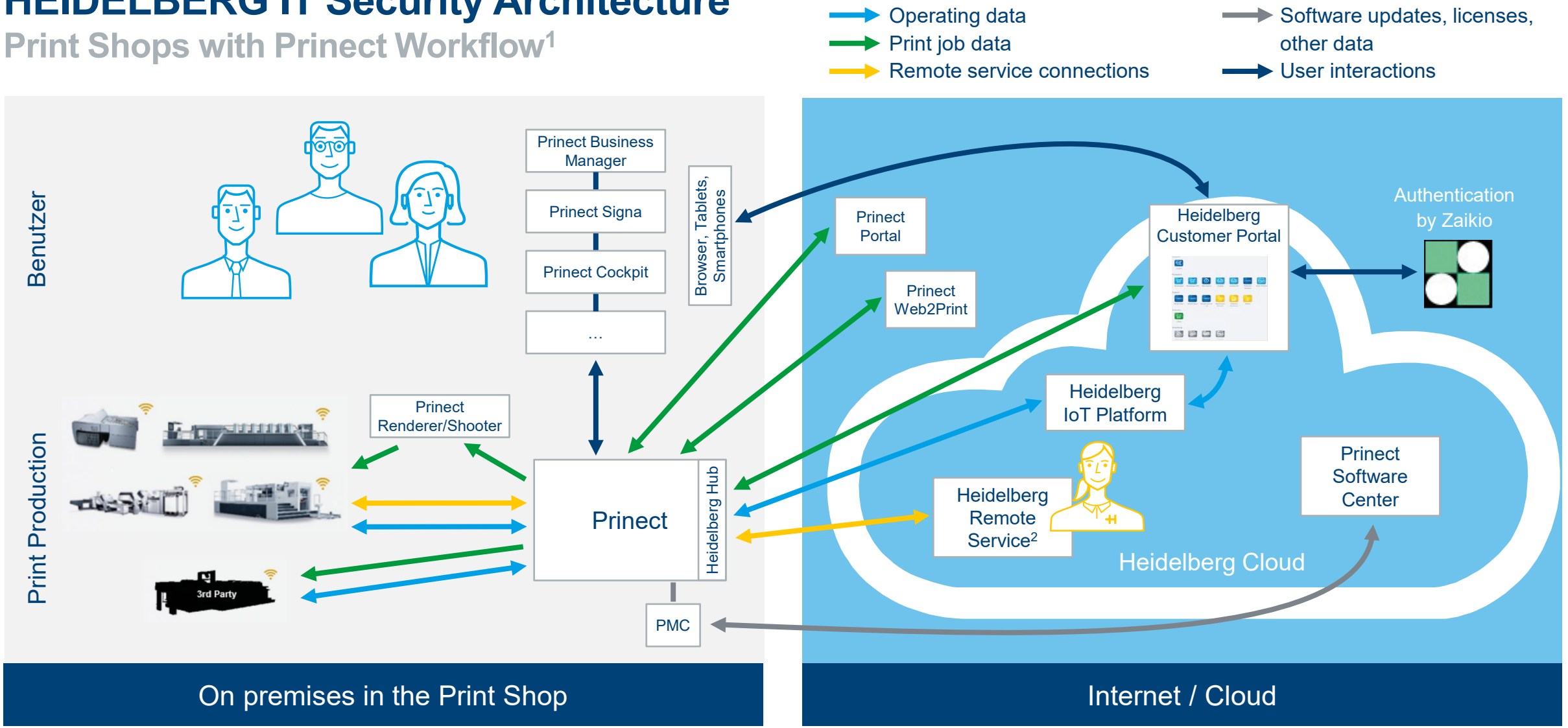
Heidel-berger Druck

Third Party (Cloud Service Provider etc.)

	On Premises in the Print Shop	HEIDELBERG Cloud (Software as a Service)
Customer Data	Operating and production data, print job data, customer master data, material data, user data, organizational data, etc.	
Application Operational Security	distributed Software (Prinect, Device Software etc.)	
Application/Platform Operational Security		HEIDELBERG Customer Portal, HEIDELBERG IoT Platform, Remote Service…
Security of Distributed Software	Prinect, DFEs, etc.	
Application Security		HEIDELBERG Customer Portal, HEIDELBERG IoT Platform, Remote Service…
Security of the Machines/IoT Devices	Printing Machines, Post-Press Machines, CtP Devices, etc.	
Platform Security		
Operation System Security		
Network Security		
Security of Virtualized Infrastructure		
Physical Infrastructure Security	Hardware, Data Center, Buildings, etc.	
Physical Infrastructure Security		Hardware, Data Centers, Buildings, Regions, etc.

HEIDELBERG IT Security Architecture

Print Shops with Prinect Workflow[1]



[1] Prinect Production Manager, Prinect Production System, Pressroom Manager, Prepress Manager, Integration Manager; all at least from software version 21.10

[2] if maintenance contract exists

There is no such thing as 100% security

"The only truly secure system is one
that is powered off,
cast in a block of concrete and
sealed in a lead-lined room with armed guards
– and even then I have my doubts."

Gene Spafford

Thank you very much for your attention!