


To receive SHRM code for the recertification credit and HRCI self-submission instructions, plan to attend all 60 minutes of this webinar.

Insight


This program is valid for 1 PDC toward SHRM-CP and SHRM-SCP recertification.


This activity can be self-submitted for 1 HR (General) recertification credit hours toward aPHR™, PHR®, PHRca®, SPHR®, GPHR®, PHRI™ and SPHRI™ recertification through HR Certification Institute® (HRCI®). For more information about certification or recertification, please visit the HR Certification Institute website at www.hrci.org.

1

1






thread
Insight

The Intersection of HR and Information Security

Presented by
Eric T. Cook, SPHR, SHRM-SCP

2

2





Agenda

- Intro
- Records Retention and Disposal
- Systems We Manage (or not)
- People: The Easiest Hack
- Quick Tips, and Q & A


3

3



Intro

4




Why It Matters Now

There has never been a better or more lucrative time to steal or attempt to steal HR and employment records.

5

5




Simplified Glossary

- **Hacking:** Exploiting systems with bugs and other techniques to break in
- **Phishing/Spoofing:** Attempting to obtain information through impersonation
- **Ransomware:** Tools that lock a network, computer, or account
- **Malware/Spyware:** Hidden software that causes harm or grants unwanted access
- **Virus/Worms:** Self-spreading malicious software or code
- **Denial of Service (DOS) attack:** Repeated visits intended to crash a server
- **Social Hacking/Engineering:** Attempting to manipulate users into granting access

6

6




Encryption and Why It Matters

- Encryption is simply encoding a message or information
- The goal is to ensure that only authorized parties access information
- An encrypted message or information is essentially turned into gibberish
- That gibberish can then be translated into the actual contents with a “cypher” or code


7

7



Records, Retention, and Disposal

8



Sensitivity of HR Records


More sensitive ↑

- Health records and similar certifications
- W-2, W-4, I-9 and similar forms
- Anything with social security numbers
- Benefits and retirement enrollment forms
- Pay stubs and pay statements
- Job applications and resumes
- Phone directories
- Job descriptions and other employer-centered records

↓ Less sensitive

9

9



Where Do HR Records Reside?

- Physical folders, drawers, binders or piles
- Local hard drives and phones
- Online internet accessed private or shared drives
- Online HR, payroll, benefits information systems

10

10




Paper and Physical Files

- Follow record retention guidelines
- Shred documents that you are no longer legally required to retain or that are not subject to retention (*be careful here*)
- Never place HR-related items in the garbage or recycling

11

11

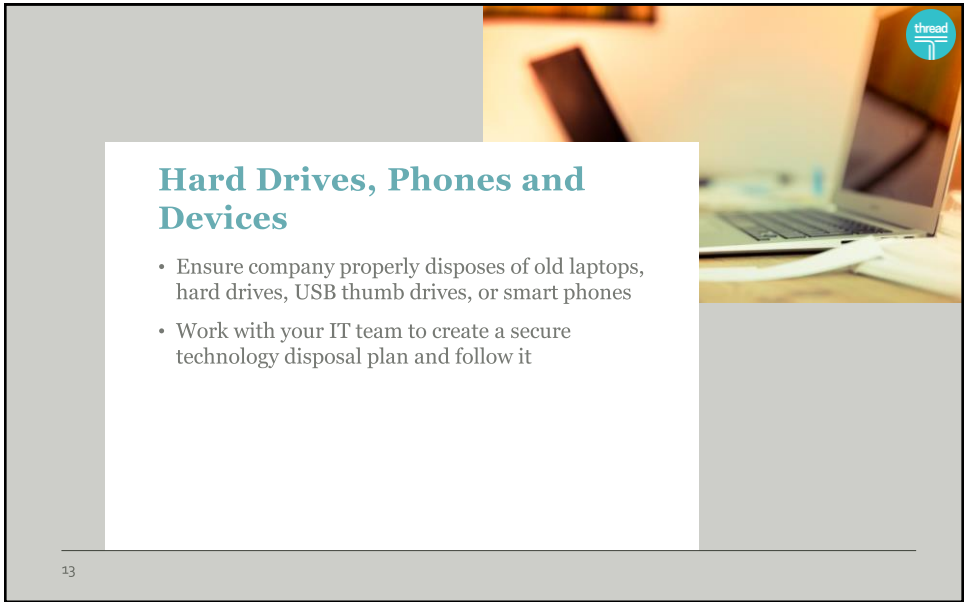


How Should Physical HR Records Be Secured?

- Locked files or rooms (ideally both)
- Consider the type of record and how sensitive it is
- HIPAA and banking records may have their own rules

12

12

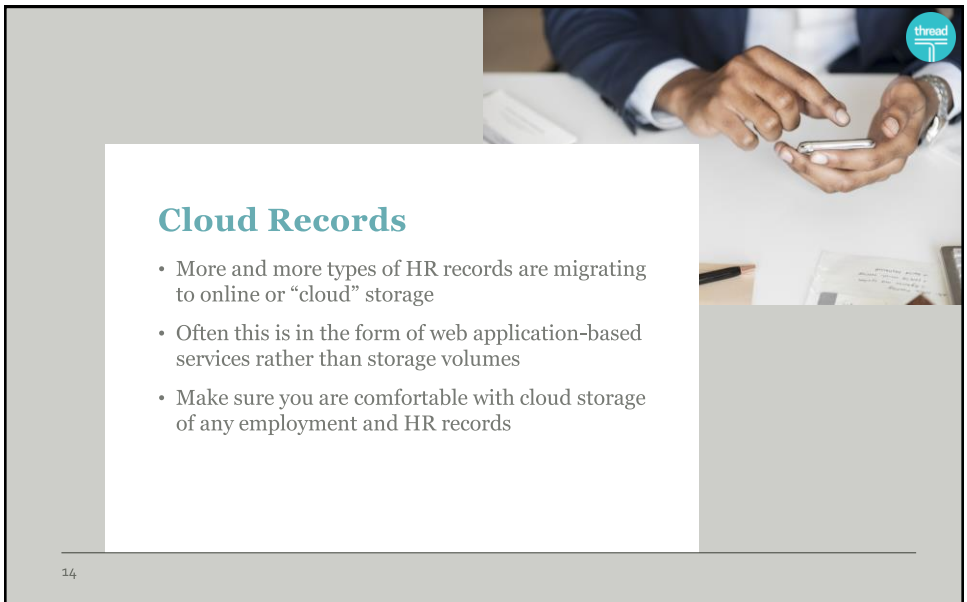


Hard Drives, Phones and Devices

- Ensure company properly disposes of old laptops, hard drives, USB thumb drives, or smart phones
- Work with your IT team to create a secure technology disposal plan and follow it

13

13





Cloud Records

- More and more types of HR records are migrating to online or “cloud” storage
- Often this is in the form of web application-based services rather than storage volumes
- Make sure you are comfortable with cloud storage of any employment and HR records

14

14





Records Retention and Cloud Records

- Can electronic cloud records be destroyed? (probably not)
- Are there tools to automate records retention? (usually not)
- How easy is it to migrate your HR records?

15

15




Ideal HR Records Separation

File	Individually	All Together	Special
Personnel file	X		
I-9 files		X	
Medical/confidential file	X	X	
Payroll record file	X	X	
Workplace injury file	X	X	Case specific

16

16



Records Retention

- Records retention will depend on the individual records.
- For most records seven years after termination is a safe record retention period.

Cheat Sheet

- *Wage records*: 3-4 years
- *Tax records*: 4 years
- *Resumes of non-hired applications*: 1 year (2 for Federal Contractors)
- *Form I-9s*: unique periods
- *Information about toxic substance exposure*: 30 years
- *ERISA records*: often 6 years

17

17

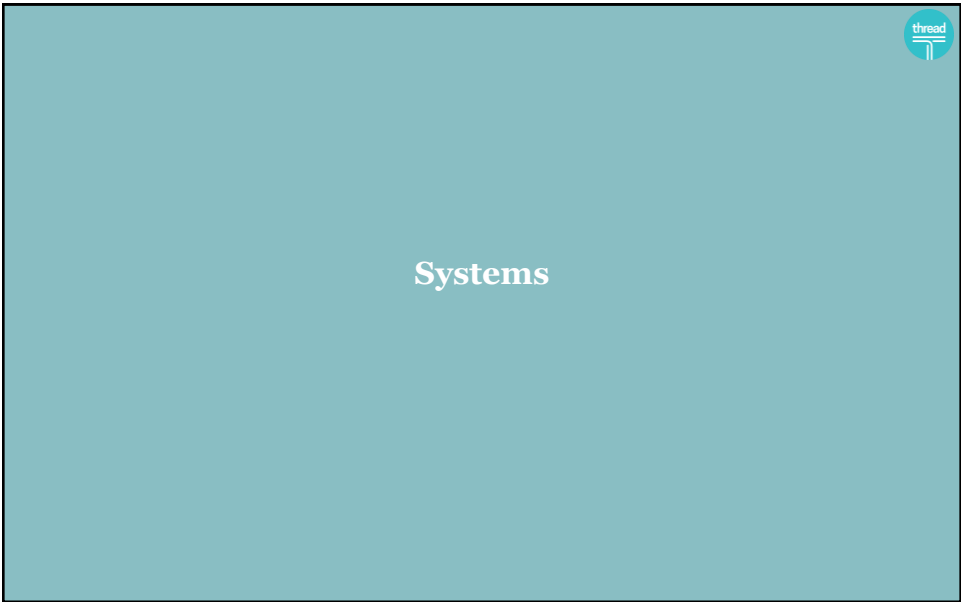


Record Separation and Online Records

- Are files divided between sub folders?
- I-9 Employment Eligibility Verification forms
- Audits and investigations

18

18




19

Avenues of Attack




Email, HRIS access, network intrusion, mobile phones, computers, accounts and web applications, internet enabled devices, vendors and service providers, etc.

20

20






Different Online Systems

-  **Employer-hosted storage**
(A local shared hard drive that employees can access remotely)
-  **Cloud shared drives by outside services**
(Microsoft OneDrive, Google Drive)
-  **Web application services and the data they maintain or store**
(Your web application tracking system or similar site)

21

21




Different Systems, Different Risks

- Physical drives and files can be lost or stolen
- Shared cloud drives are often not encrypted and entire volumes can be accessed or stolen
- Data stored or held through online services are often more secure and usually mostly or fully encrypted and part of a larger pool

22

22




Other Vulnerabilities in Work Tools

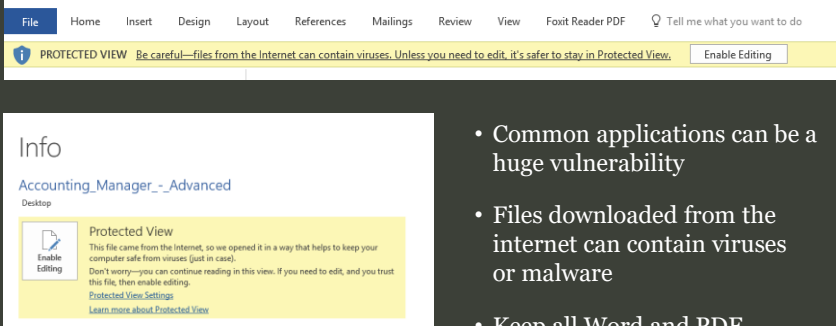
- Word processing and document
- Spreadsheets
- Email programs
- Internet-enabled devices

23

23



Word and PDF Vulnerabilities



- Common applications can be a huge vulnerability
- Files downloaded from the internet can contain viruses or malware
- Keep all Word and PDF applications updated

24


24

Back Up All Files

- Plan as if your hard drive could vanish at any moment
- Don't rely solely on encryption
- Back up databases frequently
- Watch out for ransomware attacks

Legitimate-Looking Alert

WARNING
Your Computer is Encrypted.

Please kindly pay 1,000  *bitcoin* to unlock your files.

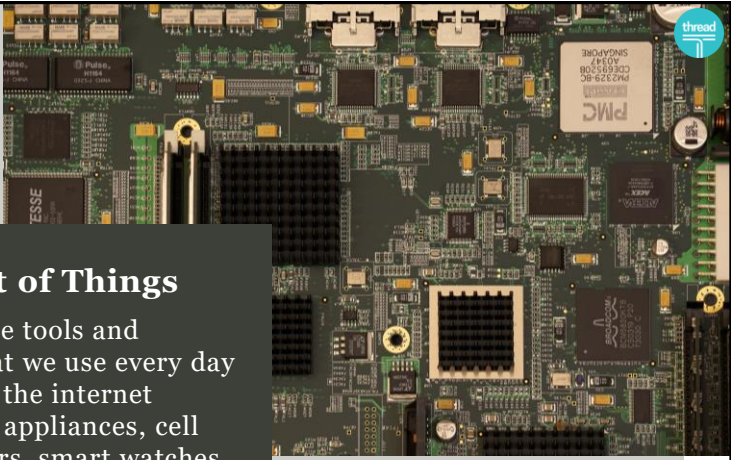
[Click Here to Let Us Steal Your Money and Info](#)

25

25

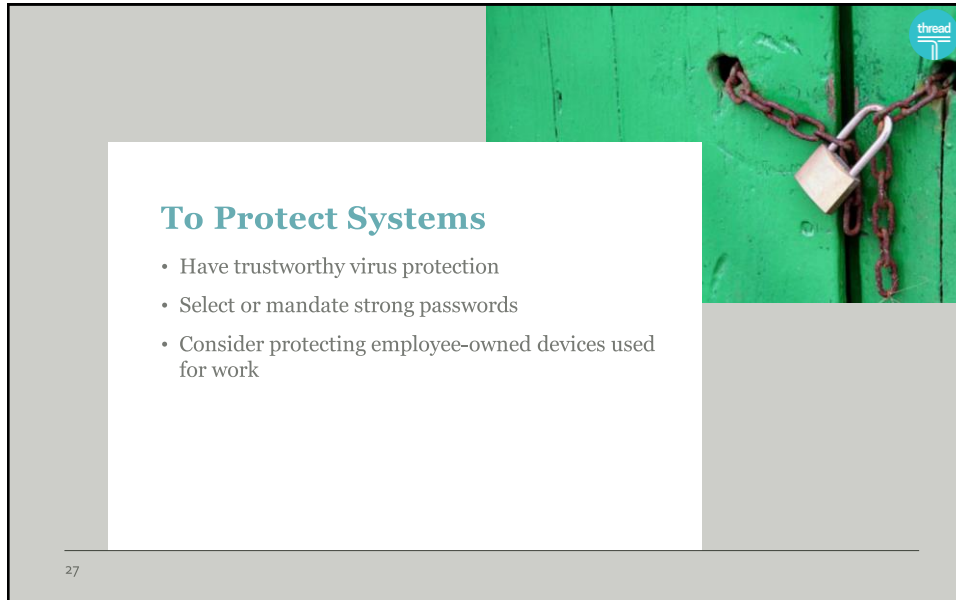
Internet of Things

Many of the tools and devices that we use every day connect to the internet (e.g. home appliances, cell phones, cars, smart watches, virtual assistants)



26

26

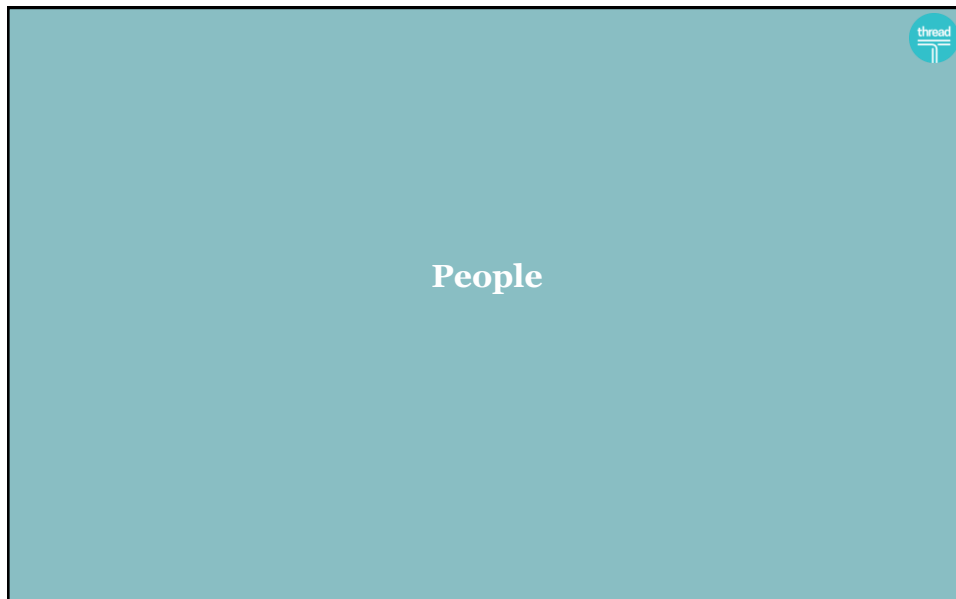


To Protect Systems

- Have trustworthy virus protection
- Select or mandate strong passwords
- Consider protecting employee-owned devices used for work


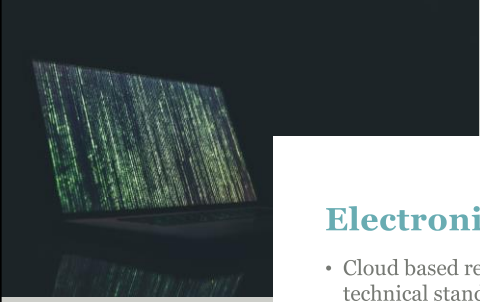
27

27



People

28




Electronic Records Access

- Cloud based records are often very secure from a technical standpoint
- Hacking into a **sophisticated** online system is fairly difficult
- Acquiring a password however is trivially easy


29


29



Two Main Ways to Access Secure Systems

Fri 3/16/2018 1:16 PM

 Info Services
WIN FREE MONEY

To  Eric Cook


Click on this link in the next 10 minutes and send us your banking information. We will wire you \$1,000,000 dollars

Don't miss this fruitful opportunity: <http://bankusa.co/hrfg-f44q/>


1. Defeating security features to break into a secure system
2. Deceiving a target into granting access to a secure system


30


30




HR is the Gateway





 Hacker


 HR Team



 Sensitive Data

31

31



Phishing Scams



Fri 3/10/2017 2:15 PM

✓ Celine Houston, CEO

Urgent Files – Highest Priority

To ● Eric Cook

Hello Eric,



Pleased send me all w-2 records for current & former employees for last year. Please reply by end of day and cc my new consultant "ceoinfomationervices@5v.info"

Thank you for your prompt attention.
CEO

If you ever receive a similar email, don't respond! It's likely a scam.

32

32




Case Study

Jarett, a Program Coordinator at Smith Industries, receives an email from the CEO asking him to purchase 25 iTunes gift cards with \$50 loaded to each and to email back all of the codes. Jarett complies with the request and replies with all 25 gift card numbers.

What do you think about this?

33

33

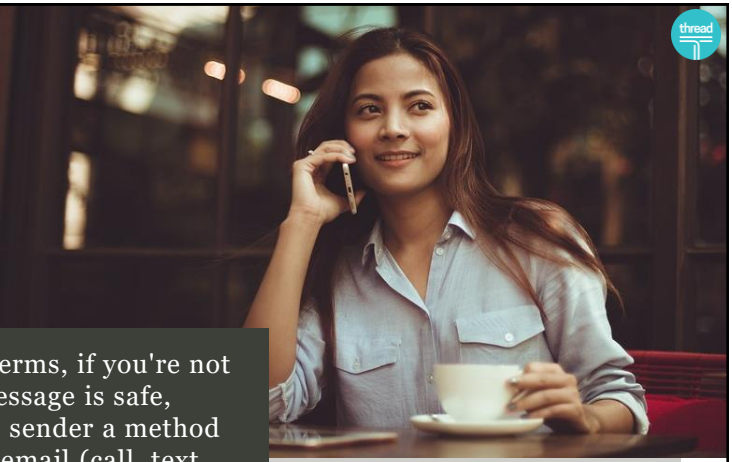


Ways Email Can Go Wrong

- Sending to the wrong person or an outside party
- Inadvertent or malicious forwarding
- “Spoofed” or fake sender/recipient who is not who they claim to be
- Local or global system hack or malware

34


34



In simple terms, if you're not sure if a message is safe, contact the sender a method other than email (call, text, etc.) for clarification.

35

35




Train Employees

- Add information about security guidance to onboarding
- Ensure current employees are aware of best practices on information security
- Have policies in place—and follow them

36

36




Top Three People Tips

- 1** Don't divulge sensitive records to anyone unless you know who they are and why they have a legitimate right to access the files.
- 2** Don't send sensitive information through unsecured email.
- 3** Train employees on the basics of electronic security, especially those who have access to sensitive records.


37

37



Quick Tips and Q&A

38





Quick Tips

- Back up your digital files and make sure they are secure
- Update programs and virus protection regularly
- Use encryption whenever possible
- Create strong passwords (6+ characters with mix of letters, numbers, and symbols)
- Create and follow a secure document and device destruction process
- Never email sensitive information, like employee SSNs or login credentials
- Never click links that look suspicious, even from a source you trust



39

39



Q & A

40

Eric T. Cook

SPHR, SHRM-SCP | Associate Director of HR Services

Eric has extensive experience presenting, teaching and implementing great HR practices. He was honored as a Runner-Up Award winner in the first ever Portland Business Journal HR Leadership Awards. During his career, he has held several senior HR positions, including the HR & Operations Manager for an award-winning interactive marketing agency and as HR Director for a prestigious law firm. Additionally, Eric brings valuable experience from his work with publicly traded companies, professional services firms, government agencies, and non-profits.

41



41

If you attended the full 60-minute webinar, the SHRM recertification code and HRCI self-submission instructions will be emailed to you.

Insight

This program is valid for 1 PDC toward SHRM-CP and SHRM-SCP recertification.

This activity can be **self-submitted** for 1 HR (General) recertification credit hours toward aPHR™, PHR®, PHRca®, SPHR®, GPHR®, PHRI™ and SPHRI™ recertification through HR Certification Institute® (HRCI®). For more information about certification or recertification, please visit the HR Certification Institute website at www.hrci.org.

The Intersection of HR and Information Security

HR professionals deal with more risk and more scrutiny than ever when it comes to sensitive information. Join us for a deeper dive into the interaction of HR practices and information security, with a focus on essential practices and other useful hints. We will discuss ongoing requirements to safeguard employees' private personal information and the role that HR plays in strengthening an organization's information security. The session will also talk in broad terms about data breaches and how HR can help prevent them.

42

42