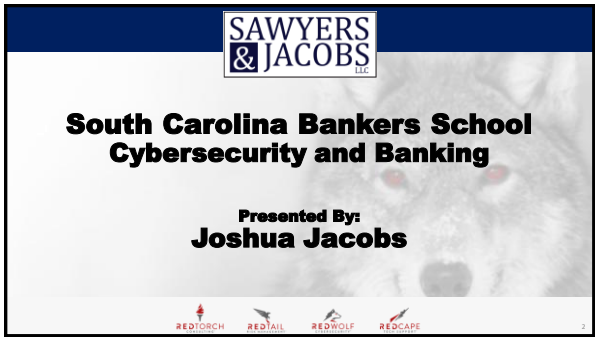

SAWYERS & JACOBS LLC
REDWOLF
CYBERSECURITY™
REDTORCH
REDTAIL
REDWOLF
REDCAPE

1


SAWYERS & JACOBS LLC
South Carolina Bankers School
Cybersecurity and Banking
Presented By:
Joshua Jacobs
REDTORCH
REDTAIL
REDWOLF
REDCAPE

2


SAWYERS & JACOBS LLC
Banking and
Cybersecurity
REDTORCH
REDTAIL
REDWOLF
REDCAPE

3

Joshua Jacobs

Joshua Jacobs has over twenty years of experience providing information technology consulting services and solutions focusing on financial institutions. He is an Indiana University Kelly School of Business graduate with a Master of Science in Finance (MSF) and a Christian Brothers University graduate with a Master of Business Administration (MBA), a Bachelors of Science in Business Administration with a concentration in Information Technology Management, and a Graduate Certificate in Project Management (GCPM).

He is currently serving as an adjunct faculty member at his alma mater, Christian Brothers University, teaching a course on Digital Forensics that is part of the Cybersecurity & Digital Forensics degree program. He holds numerous IT and IT security certifications including the Certified Information Systems Security Professional (CISSP), the GIAC Penetration Tester (GPEN), and the Systems Security Certified Practitioner (SSCP). He is also the co-author of the SSCP Study Guide and DVD Training System. He specializes in cybersecurity assessments and penetration testing, network design and support, and network virtualization.

www.sawyersjacobs.com
© 2026 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

4

4

Class Topics

- ❑ Cybersecurity Lingo
- ❑ The Regulatory Environment
- ❑ Cybersecurity in the News
- ❑ Case Studies of Real-World Cybersecurity Events

www.sawyersjacobs.com
© 2026 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

5

5

Information Security Defined

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction

Source: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

www.sawyersjacobs.com
© 2026 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

6

Confidentiality, Integrity, & Availability (CIA)

Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Source: *FIPS Publication 199, February 2004, Computer Security Division, National Institute of Standards and Technology (NIST)*

www.sawyerjacobs.com
© 2008 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

7

Confidentiality, Integrity, & Availability (CIA)

Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Source: *FIPS Publication 199, February 2004, Computer Security Division, National Institute of Standards and Technology (NIST)*

www.sawyerjacobs.com
© 2008 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

8

Confidentiality, Integrity, & Availability (CIA)

Availability - Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Source: *FIPS Publication 199, February 2004, Computer Security Division, National Institute of Standards and Technology (NIST)*

www.sawyerjacobs.com
© 2008 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

9

Why is Cybersecurity Important

Customers expect us to protect their money and their information

PII is "any information about an individual maintained by an agency, including

(1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and

(2) any other information that is linked or linkable to an individual, such medical, educational, financial, and employment information."

Source: NIST SP-800-12 (Guide to Protecting the Confidentiality of PII)

www.sawyerjacobs.com
© 2026 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

10

The Balancing Act

www.sawyerjacobs.com
© 2026 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

11

11

Risk Recognition

Comptroller's Handbook:

"The OCC recognizes that banking is a business of assuming risks in order to earn profits."

www.sawyerjacobs.com
© 2026 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

12

12

Function of IT

Information Technology is a means to an end to support the bank's strategic goals.

13

Assessing Risk

"According to MPD, the suspects did not get any money because employees emptied the ATM on Sunday. The property damage is approximately $40,000.

Officers found several tools, including a crowbar and screwdriver, in the parking lot."

Source: https://wreg.com/news/local/atm-ripped-from-wall-at-cordova-bank/

14

Texas ATM Jackpotting

March 18, 2025

- Nearly $236,000 stolen over four days
- Targeted more than 70 ATMs across Texas including Houston, Dallas, Austin, and San Antonio
- Attacked ATMs at gas stations and other small businesses
- Seven charged, and five not identified
- Alleged ringleader on humanitarian visa and faces similar charges in Georgia and Florida

https://www.click2houston.com/news/local/2025/03/19/texas-atms-hacked-in-sophisticated-jackpotting-theft-scheme-with-ties-to-russia/

15

Texas ATM Jackpotting

March 18, 2025

- Attackers seen obtaining recent receipts and then using cell phones to communicate with someone else
- ATMs tricked into thinking transaction was cancelled and no account was debited even though ATM dispensed money
- Records indicate suspects at ATMs get 30% and ringleader gets 70%

https://www.click2houston.com/news/local/2025/03/19/texas-atms-hacked-in-sophisticated-jackpotting-theft-scheme-with-ties-to-russia/

www.sawyersjacobs.com
© 2026 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

16

16

Jackpotting Methods

Method #1: Malware Jackpotting

Malware introduced to the ATM/ITM hard drive via USB or by physically introducing to the existing hard drive. Uses the existing ATM/ITM computer and dispenser.

US Secret Service Alert: https://files.constantcontact.com/6e263713201/3bb6fb95-7a7a-4aa5-bb9e-e60dfc7add84.pdf?rdr=true

www.sawyersjacobs.com
© 2026 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

17

17

Jackpotting Methods

Method #2: Black Box Jackpotting

ATM/ITM dispenser is disconnected from the original computer and connected to an unauthorized device (e.g., laptop or tablet) to send commands to the dispenser.

US Secret Service Alert: https://files.constantcontact.com/6e263713201/3bb6fb95-7a7a-4aa5-bb9e-e60dfc7add84.pdf?rdr=true

www.sawyersjacobs.com
© 2026 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

18

18

Jackpotting Methods

Method #3: RMS/Man-in-the-Middle Attacks

Targets the software used by ATMs to communicate with the host system to instruct ATM to dispense cash without debiting any account.

US Secret Service Alert: https://files.constantcontact.com/6e263713201/3bb6fb95-7a7a-4aa5-bb9e-e60dfc7add84.pdf?rdr=true

www.sawyersjacobs.com
© 2026 Sawyers & Jacobs LLC

19

Jackpotting Protections

Protecting Against Attack Method 3:

1. Disable remote and wireless access to RMS
2. Use physical firewall to limit access to only required hosts
3. Change default passwords and PINs
4. Encrypt all traffic with Transport Layer Security (TLS)

www.sawyersjacobs.com
© 2026 Sawyers & Jacobs LLC

20

Jackpotting Protections

Protecting Against Attack Methods 1 and 2:

1. Change locks to outside cabinet so that master keys cannot be used to access ATM/ITM computer
2. Consider alarms for access to computer cabinet in addition to cash cabinet
3. Encrypt ATM/ITM computer hard drives
4. Consider disabling USB ports
5. Keep operating system and software patched

www.sawyersjacobs.com
© 2026 Sawyers & Jacobs LLC

21

Top 13 Risk Assessments

1. Gramm-Leach-Bliley Act (GLBA) Information Security
2. Electronic banking and online services
3. Remote Deposit Capture (RDC)
4. Enterprise Risk Assessment (ERA)
5. Information Technology (IT)
6. ID Theft/Red Flags
7. Business Continuity Planning (BCP)
8. Vendor Management
9. Internal Controls
10. Mobile Banking
11. Social Media
12. Corporate Account Takeover (CATO)
13. Cybersecurity Risk Assessment

www.sawyersjacobs.com
© 2026 Sawyers & Jacobs LLC

22

Risk Assessments

"All models are wrong; some models are useful."

- George E. P. Box

www.sawyersjacobs.com
© 2026 Sawyers & Jacobs LLC

23

Assessing Risk

- **Threat** - anything that has the potential to cause harm.
- **Risk** - the likelihood that something harmful will occur and will have an impact on the bank's achievement of its objectives. Risk is measured in terms of likelihood and impact.
- **Likelihood of Occurrence** - the probability that a threat will occur. A threat may be ***possible*** but is it ***probable***?
- **Magnitude of Impact** - the extent of damage, or how bad it will hurt, are two ways to define magnitude of impact.

www.sawyersjacobs.com
© 2026 Sawyers & Jacobs LLC

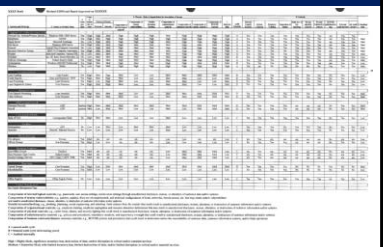
24

Assessing Risk

25

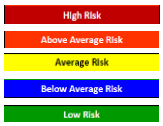
How NOT to create a risk assessment

- Don't make it too complicated
- Reach a conclusion
- Does it make sense?



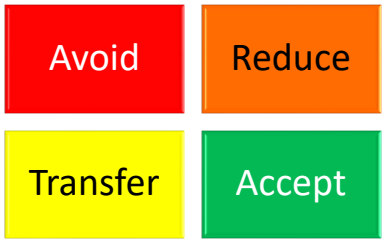
26

The Power of Color-Coding Risk



27

Risk Responses



28

Avoid

Exit the area presenting the risk. Risk avoidance could involve shutting down a line of business, closing an office, leaving a geographical market, or selling a branch or division.

29

Reduce

Take action to reduce the probability of the threat occurring or the magnitude of impact should it occur. This is normally accomplished through mitigating controls.

30

Transfer

Share a portion of the risk by buying insurance, outsourcing an activity, or hedging.

www.sawyerjacobs.com
© 2026 Sawyers & Jacobs LLC

31

Accept

Take no action. Accept the risk as a normal part of doing business.

www.sawyerjacobs.com
© 2026 Sawyers & Jacobs LLC

32

Black Swan Events

- Low Probability
- High Impact
- Unexpected
- Can be positive or negative
- Causes massive consequences
- Risk assessment models are not helpful for such events
- Scenario analysis is much more prudent

www.sawyerjacobs.com
© 2026 Sawyers & Jacobs LLC

33

Is the CAT Useful?

FFIEC

Cybersecurity Assessment Tool

May 2017

https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf

34

Ransomware Self Assessment Tool (2.0)

Bankers Electronic Crimes Task Force | CSBS | U.S. Department of Homeland Security United States Secret Service

Ransomware Self-Assessment Tool (R-SAT)

October 24, 2023
Version 2.0

Developed in collaboration with the Bankers Electronic Crimes Task Force, State Bank Regulators, and the United States Secret Service

35

The Tech Landscape

- Servers
- Network Devices
- Services, Ports
- Ports

36

Vulnerabilities and Exploits

37

Patches

38

All Vulnerabilities Are Not Created Equally

CRITICAL Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)

Description

The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.

Solution

Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N /UI:N/S:U/C:H/I:H/A:H

CVSS Base Score: 10.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

39

Social Engineering

The practice of obtaining confidential information through social interaction (e.g., phone call, email, in-person conversation, online forms)

www.sawyerjacobs.com
© 2016 Sawyers & Jacobs LLC
REDTORCH REDTAIL REDWOLF REDCAPE

40

Phishing

Phishing – using email messages to trick people into giving up personal, confidential information such as passwords, PINs, credit card information, social security numbers, etc.

www.sawyerjacobs.com
© 2016 Sawyers & Jacobs LLC
REDTORCH REDTAIL REDWOLF REDCAPE

41

Phishing Frequency and Results

www.sawyerjacobs.com
© 2016 Sawyers & Jacobs LLC
REDTORCH REDTAIL REDWOLF REDCAPE

42

Anyone can be tricked!

www.sawyerjacobs.com
© 2026 Sawyers & Jacobs LLC

43

Evolution of Security Monitoring

- Intrusion Detection System → Intrusion Prevention System (IPS)
- Security Information and Event Management (SIEM)
- Internal Monitoring → Monitoring by 24/7 Security Operations Center (SOC)
- Managed Security Services Provider (MSSP) → Managed Detection and Response (MDR) Provider, which could include:
  - Threat hunting and detection response versus only monitoring
  - Might deploy/manage/monitor Endpoint Detection and Response (EDR) agents.
  - Might deploy honeypots to internal network

www.sawyerjacobs.com
© 2026 Sawyers & Jacobs LLC

44

44

Evolution of Security Monitoring

MDR Provider

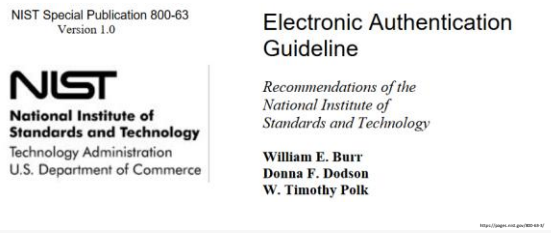
- Threat hunting and detection response versus only monitoring
- Might deploy/manage/monitor Endpoint Detection and Response (EDR) agents.
- Might deploy honeypots to internal network

www.sawyerjacobs.com
© 2026 Sawyers & Jacobs LLC

45

45

Guidance


NIST Special Publication 800-63
Version 1.0

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Electronic Authentication Guideline

Recommendations of the National Institute of Standards and Technology

William E. Burr
Donna F. Dodson
W. Timothy Polk

https://pages.nist.gov/800-63-3/

www.sawyerjacobs.com
© 2026 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

46

46

NIST 800-63 (Updated June 22, 2017)

- Definitions
  - Memorized Secret: Passwords, passphrases, or PINs
  - Credentials Service Provider (CSP): A trusted entity that issues electronic credentials
- What it DOESN'T specifically say – Increase password length from 8 characters to 11, 14, or more characters

https://pages.nist.gov/800-63-3/

www.sawyerjacobs.com
© 2026 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

47

47

NIST 800-63 (Updated June 22, 2017)

PASSWORD AGING

SP 800-63B (Section 5.1.1.2)

"Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator."

https://pages.nist.gov/800-63-3/

www.sawyerjacobs.com
© 2026 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

48

48

NIST 800-63 (Updated June 22, 2017)

PASSWORD COMPLEXITY

SP 800-63B (Section 5.1.1.2)

"Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets."

https://pages.nist.gov/800-63-3/

www.sawyerjacobs.com
© 2026 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

49

NIST 800-63 (Updated June 22, 2017)

PASSWORD LENGTH

SP 800-63B (Section 5.1.1.1)

"Memorized secrets SHALL be at least 8 characters in length if chosen by the subscriber. Memorized secrets chosen randomly by the CSP or verifier SHALL be at least 6 characters in length and MAY be entirely numeric."

https://pages.nist.gov/800-63-3/

www.sawyerjacobs.com
© 2026 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

50

NIST 800-63 (Updated June 22, 2017)

- Caveats
  - "…recommend increased length as a key password security control, especially through encouraging the use of passphrases."
  - "…recommended that passwords chosen by users be compared against a "black list" of unacceptable passwords. This list should include passwords from previous breach corpuses, dictionary words, and specific words (such as the name of the service itself) that users are likely to choose."
  - "Highly complex memorized secrets introduce a new potential vulnerability: they are less likely to be memorable, and it is more likely that they will be written down or stored electronically in an unsafe manner. While these practices are not necessarily vulnerable, statistically some methods of recording such secrets will be."

https://pages.nist.gov/800-63-3/

www.sawyerjacobs.com
© 2026 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

51

Microsoft Security Baseline

- Windows 10 v1903 and Windows Server v1903
- Draft released April 24, 2019 with final released May 23, 2019
- Includes dropping password-expiration policies that require periodic password changes.

https://blogs.technet.microsoft.com/secguide/2019/05/23/security-baseline-final-for-windows-10-v1903-and-windows-server-v1903/

52

Passwords on the Web

- What can we find on the web?

53

Multifactor Authentication (MFA)

- Something you KNOW
- Something you HAVE
- Something you ARE

MFA must use two of the three

54

MFA for Internal Accounts?

- Insurance requirements and examiner recommendations are pushing multifactor for internal accounts.
- Good control, but not a panacea

55

Password Hashes

- MFA authentication is typically a layer on top of integrated password hashes.
- Since hashes still exist, capturing and using them directly could still be an available.
- Hashes can be cracked offline to obtain the passwords.

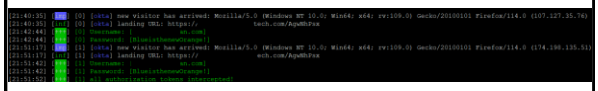
56

Man-in-the-Middle (MITM) Attack

- Active Method used to bypass MFA on cloud services
- All traffic flows through “attackers” machine
- Capture username, password, and authentication token

57

Man-in-the-Middle (MiTM) Attack



58

The "Cloud"

- What is the Cloud?
- On-Premise or Off-Premise
- Common cloud services used in banks
- Cloud Access Security Broker (CASB)

59

Examiner Notification

- November 23, 2021, the FDIC, Federal Reserve, and OCC issues joint statement on computer-security incident notification requirements.
- Full compliance for banks and bank service providers is May 1, 2022.
- FDIC banks can report incident to case manager or incident@fdic.gov

https://www.fdic.gov/news/financial-institution-letters/2022/fil22012.html

60

Examiner Notification

Page 8 contains a "… non-exhaustive list of incidents that generally are considered 'notification incidents' under the new rules:

1. Large-scale distributed denial of service attacks that disrupt customer account access for an extended period of time (e.g., more than 4 hours);
2. A bank service provider that is used by a banking organization for its core banking platform to operate business applications is experiencing widespread system outages and recovery time is undeterminable;
3. A failed system upgrade or change that results in widespread user outages for customers and banking organization employees;
4. An unrecoverable system failure that results in activation of a banking organization's business continuity or disaster recovery plan;
5. A computer hacking incident that disables banking operations for an extended period of time;
6. Malware on a banking organization's network that poses an imminent threat to the banking organization's core business lines or critical operations or that requires the banking organization to disengage any compromised products or information systems that support the banking organization's core business lines or critical operations from internet-based network connections; and
7. A ransom malware attack that encrypts a core banking system or backup data."

https://www.fdic.gov/news/financial-institution-letters/2022/fil22012.html

www.sawyersjacobs.com
© 2026 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

61

61

SAWYERS & JACOBS LLC

Preparing for Reviews and Exams

REDTORCH REDTAIL REDWOLF REDCAPE

62

62

The Examination

- The "standards" are applied differently from state to state and region to region.
- Reactive to the last big event.
- Requirements vary from bank to bank (e.g., IT internal audit coverage; network security).
- Communication gap between bankers and regulators; misinterpretation of exam findings.

www.sawyersjacobs.com
© 2026 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

63

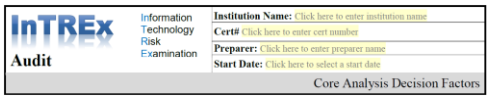
63

Compliance Versus Security

- Do not confuse "compliance" with "security"
- One can be in compliance but not secure
- Today's banks must go beyond basic compliance and practice practical risk mitigation

64

What are Examiners Looking At?



65

External Reviews

- IT Reviews
- Penetration Testing
- Vulnerability Scanning
- Cybersecurity Review

66

Misinformation and Confusion

- There is no law, regulation, guideline, or best practice that requires your bank to rotate IT Audit or Cybersecurity Assessment firms
- This is often confused with the audit partner rotation requirement of the Sarbanes-Oxley Act
- Those who suggest such rotation are misinformed and are harmful to the banking industry
- There is a shortage of qualified firms and practitioners
- Do your due diligence
- Stick with reputable firms with competent professionals

www.sawyerslacobs.com
© 2026 Sawyers & Jacobs LLC

67

Misinformation and Confusion

- What standards should be followed (NIST, CIS, FFIEC)?
- What should the scope cover?
- Is this an audit or a review?
- Workpaper availability

www.sawyerslacobs.com
© 2026 Sawyers & Jacobs LLC

68

Examining Two Types of Attacks

- Ransomware
- Business Email Compromise (BEC)
  Bank-Side and Customer-Side (CATO)

www.sawyerslacobs.com
© 2026 Sawyers & Jacobs LLC

69

69

Evolution of Ransomware

Traditional / Automated Ransomware Attacks

- Automatically deployed by end-user action or automatically detected vulnerability
- Typically encrypts a single machine or files that the user can access (e.g., network file share)

70

Evolution of Ransomware

Next-Generation

- More sophisticated in nature, generally not automated
- Targeted towards environment to maximize damage
- Goal of encrypting entire network environments and/or stealing data

71

Backups at Risk

Be aware that some attackers are now corrupting the backups *before* launching the ransom request, effectively taking option one (restore) off the table.

72

Backup Protection Terms

Air-Gapped Backups

Immutable Backups

73

File Cybersecurity Insurance Claim?

- Do you know cybersecurity policy deductible amount?
- Has management discussed a threshold to file a claim?
- Do you have a reasonable idea of consulting, legal, and replacement/reinstallation costs?
- Does the cybersecurity policy coverage include ransomware?
- Does ransomware coverage include paying the ransom?

74

Incident Response Tabletop Exercise

- Do you know cybersecurity policy deductible amount?
- Has management discussed a threshold to file a claim?
- Do you have a reasonable idea of consulting, legal, and replacement/reinstallation costs?
- Does the cybersecurity policy coverage include ransomware?
- Does ransomware coverage include paying the ransom?

75

Deepfake $25 million loss

- Finance worker of a Hong Kong multinational form was tricked into paying out $25 million
- Attended video call with several other members of staff including the company's CFO
- All other members of the call were deepfake creations
- Finance worker was suspicious after receiving email message from the company's UK-based CFO talking about a secret transaction
- Doubts were removed after having video call because all attendees looked and sounded like colleagues he recognized

https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

www.sawyersjacobs.com
© 2026 Sawyers & Jacobs LLC

76

Artificial Intelligence (AI)

- Does your Bank allow AI or prohibit its use?
- Has the Bank developed a policy to outline how AI is used in the Bank's environment?
- Has the Bank discussed the possible risks associated with various implementations of AI?

www.sawyersjacobs.com
© 2026 Sawyers & Jacobs LLC

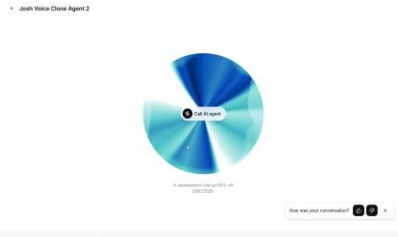
77

Cybersecurity Concerns of AI

www.sawyersjacobs.com
© 2026 Sawyers & Jacobs LLC

78

Cybersecurity Concerns of AI



https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

www.sawyersjacobs.com

REDTORCH REDTAIL REDWOLF REDCAPE

79

Case Study

Random Call, "You've been hacked"

REDTORCH REDTAIL REDWOLF REDCAPE

80

80

Case Study

Random Call, "You've been hacked"

Key Control
Is the MSSP watching?

REDTORCH REDTAIL REDWOLF REDCAPE

81

81


Case Study
CATO Event:
“But we verified”
REDTORCH
REDTAIL
REDWOLF
REDCAPE
82

82


Case Study
CATO Event:
“But we verified”
Key Control
Out-of-Band Authentication
REDTORCH
REDTAIL
REDWOLF
REDCAPE
83

83


Case Study
CATO Event:
“But we verified WITH an out-of-band method”
REDTORCH
REDTAIL
REDWOLF
REDCAPE
84

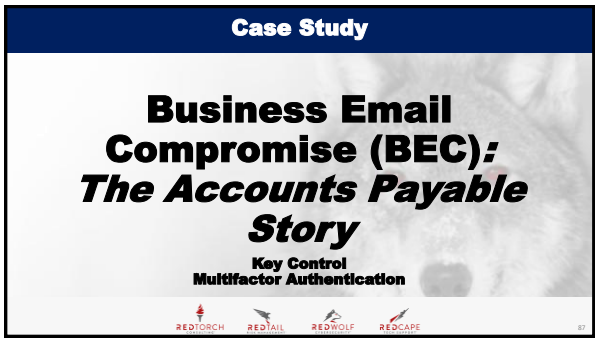
84


Case Study
CATO Event:
"But we verified WITH an out-of-band method"
Key Control
Follow call-back procedures
REDTORCH
REDTAIL
REDWOLF
REDCAPE
85

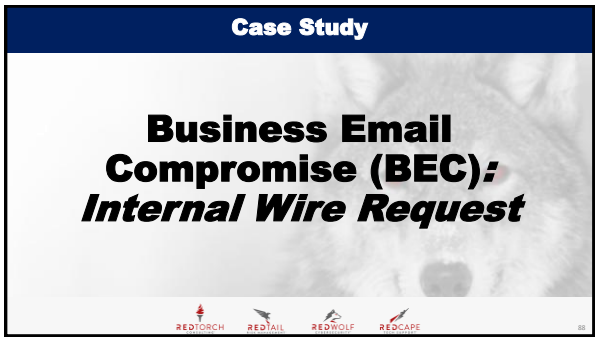
85


Case Study
Business Email Compromise (BEC): The Accounts Payable Story
REDTORCH
REDTAIL
REDWOLF
REDCAPE
86

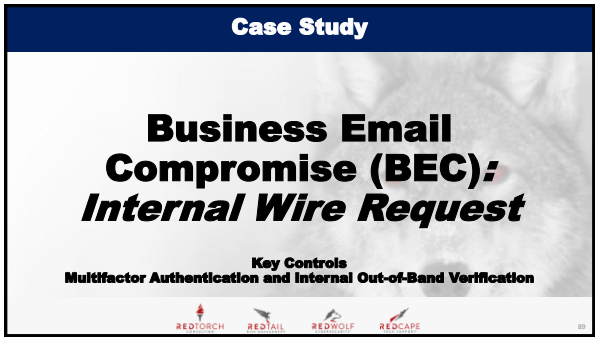
86


Case Study
Business Email Compromise (BEC): The Accounts Payable Story
Key Control
Multifactor Authentication
REDTORCH
REDTAIL
REDWOLF
REDCAPE
87

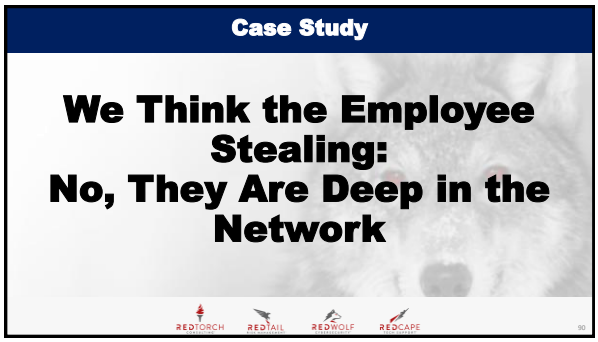
87


Case Study
Business Email Compromise (BEC): Internal Wire Request
REDTORCH
REDTAIL
REDWOLF
REDCAPE
88

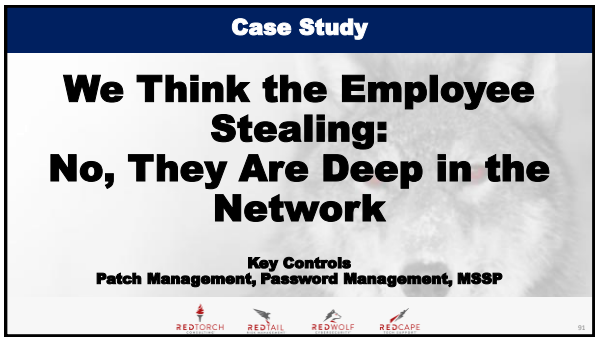
88


Case Study
Business Email Compromise (BEC): Internal Wire Request
Key Controls
Multifactor Authentication and Internal Out-of-Band Verification
REDTORCH
REDTAIL
REDWOLF
REDCAPE
89

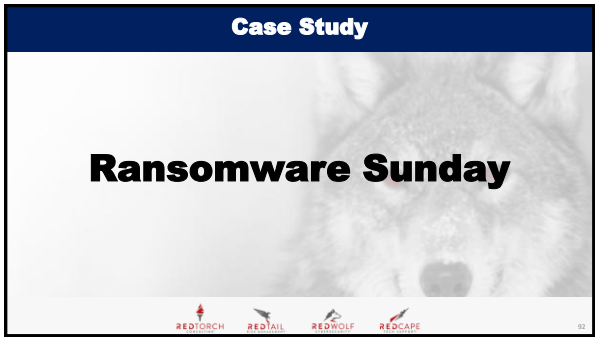
89


Case Study
We Think the Employee Stealing:
No, They Are Deep in the Network
REDTORCH
REDTAIL
REDWOLF
REDCAPE
90

90


Case Study
We Think the Employee Stealing:
No, They Are Deep in the Network
Key Controls
Patch Management, Password Management, MSSP
REDTORCH
REDTAIL
REDWOLF
REDCAPE
91

91


Case Study
Ransomware Sunday
REDTORCH
REDTAIL
REDWOLF
REDCAPE
92

92


Case Study
Ransomware Sunday
Key Controls
Vulnerability Management and Password Management
REDTORCH
REDTAIL
REDWOLF
REDCAPE
93

93

Take-Aways

- Understand that IT is a means to an end
- Protecting the bank's IT assets and customer information is critical for success
- Understand and address real risks
- Balance compliance and security

www.sawyersjacobs.com
© 2026 Sawyers & Jacobs LLC

REDTORCH REDTAIL REDWOLF REDCAPE

94

94

95