Virtual Cyber Symposium for Nonprofits & Associations 2023

Session 1: Cybersecurity 101

Chris Ecker
DelCor Technology Solutions
CTO

Darren Hulem
GRF CPA & Advisors
Manager

Andrew Leggett
DelCor Technology Solutions
Director of Cybersecurity Operations

Mac Lillard
GRF CPA & Advisors
Senior Manager

Derek Symer
AHT Insurance
Partner

Presenters

Meet the Instructors

Chris Ecker
DelCor Technology Solutions
CTO

Darren Hulem
GRF CPA & Advisors
Manager

Andrew Leggett
DelCor Technology Solutions
Director of Cybersecurity Operations

Mac Lillard
GRF CPA & Advisors
Senior Manager

Derek Symer
AHT Insurance
Partner

Agenda

- Current Landscape
- The Cybersecurity Pathway
- Technology That Helps
- IT System Triangle
- Network Security Architectures
- IT Trade-Offs
- Cyber Liability And Ransomware

Current Landscape

Recent Events

AHT INSURANCE
A BALDWIN RISK PARTNER

delcor®

grf CPAs & ADVISORS

SaaS Features

- Cloud Based Access
- Scalability
- Simple Month to Month subscription
- Simple onboarding
- 24/7 chat support
- Knowledge base articles
- Community Forum

Increase in Cyber Events

Ransomware-as-a-Service (RaaS)

Scattered Spider

Access broker

Compromises networks
Persists on systems

RDP access

Exploits

Compromised credentials

Botnets

Ransomware builder

Leak site

Payment processing

Victim messaging

RaaS operator

Develops and maintain tools

ALPHV or Alpha Spider

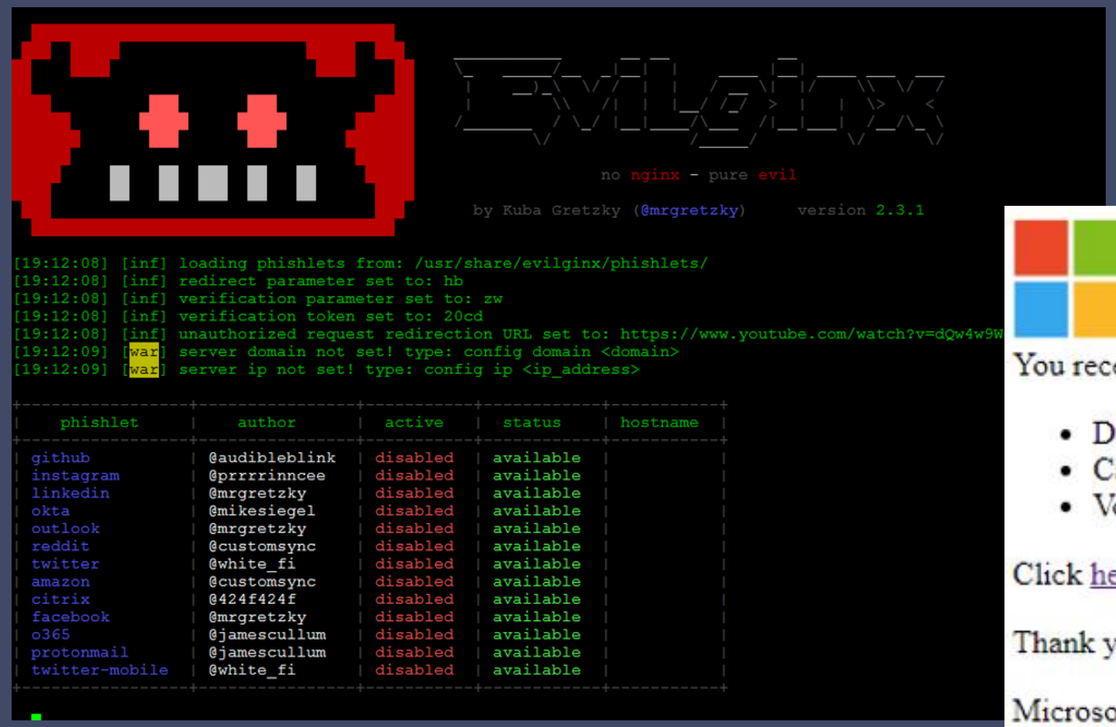
Ransomware-as-a-service affiliate

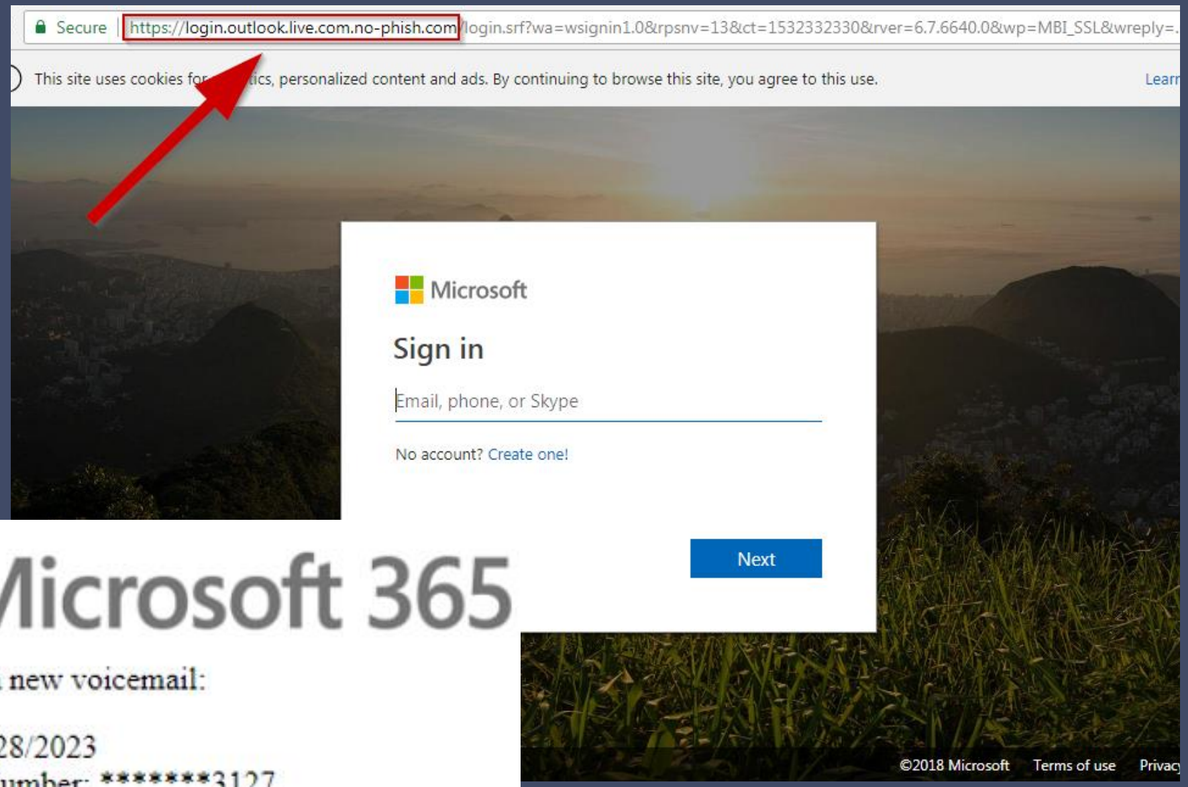
Moves laterally in network
Persists on systems
Exfiltrates data
Distributes and runs ransomware payload

Scattered Spider

Source: Microsoft & CrowdStrike

Example of Social Engineering





What Could Happen

```
[14:55:58] [imp] [0] [o365] new visitor has arrived: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
 Chrome/103.0.5060.114 Safari/537.36 Edg/103.0.1264.49 (86.82.180.135)
[14:55:58] [inf] [0] [o365] landing URL: https://login.miicrosofttonline.com/tHKNkmJt
[14:56:19] [+++] [0] Password: [-3mLhA-qzcPcUwwq62KAXMDXPyEf28q2vFe.ogRm]
[14:56:19] [+++] [0] Username: [irvins@m365x341716.onmicrosoft.com]
[14:56:19] [+++] [0] Username: [irvins@m365x341716.onmicrosoft.com]
[14:56:24] [+++] [0] Username: [irvins@m365x341716.onmicrosoft.com]
[14:56:27] [+++] [0] all authorization tokens intercepted!
[14:56:27] [imp] [0] redirecting to URL: https://portal.office.com (1)
: sessions

+-----+----------+--------------------+--------------------+----------+----------------+------------------+
| id  | phishlet |      username      |      password      |  tokens  |   remote ip    |       time       |
+-----+----------+--------------------+--------------------+----------+----------------+------------------+
| 7   | o365     | irvins@m365.....   | -3mLhA-qzcP.....   | captured | 86.82.180.135  | 2022-07-21 14:56 |
+-----+----------+--------------------+--------------------+----------+----------------+------------------+

: sessions 7

 id           : 7
 phishlet     : o365
 username     : irvins@m365x341716.onmicrosoft.com
 password     : -3mLhA-qzcPcUwwq62KAXMDXPyEf28q2vFe.ogRm
 tokens       : captured
 landing url  : https://login.miicrosofttonline.com/tHKNkmJt
 user-agent   : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.114 Safari/537.36
Edg/103.0.1264.49
 remote ip    : 86.82.180.135
 create time  : 2022-07-21 14:55
 update time  : 2022-07-21 14:56

[{"path":"/","domain":"login.microsoftonline.com","expirationDate":1689951394,"value":"0.AU4A22TlbX0IWUike5T6K2izp1tEZUfGMrBJg-Ydk3ZS
dspOAC0.AgABAAQAAAD--DLA3VO7QrddgJg7WevrAgDs_wQA9P9TJwR0XAQu0gRimpxMW5TJiTc0NERUkdTNZEj5Jj4UuyOrNgOBhKHRZz_xqjCe7KnikC_XyPWm8Q5_nJjTk
3sXkEbmZf7-67qvgHxwH2F9IKrtKfXLP6-bQ8HNELRLXZAt_jF8DeMI6ch8hcsFVEPVtZh9lskq0IjZ614wHgywqvQ1rBGa1u0C7yLqHSOKl7MQURqzwoVdMiWU9OEcYmO2IK
M7A-f3cu6nUwv0AMKwZXNDZ-ErdaTo2gyr6iNit_VQX65zhe210JKDfTrvs5s0QGQ94EUHbFJBfHuxKmoeYcWEsT9Pt0zY6_Qk2V-gogUCIdGybnDQY5GWgcF6jh113w1pQsz
2qMYN5k1vxRRh3vH3j4QiBwZWzn51_J6gzjB-Y4Dby33D30zfDiBRipVHS7uB6ZnYDbAp3d8AmS1PGW0pCg2Sr9fQ5kEbVHSfjVOhdlerS5BVFTDB5_2Mxw4BvFRIFjPD2FED
LVWCUzDk2v5_TQeRgQXqP9YfZxNg2JcX84E3Hxc_PNXTNWz4PTp9Y2l1Mq95tvHE8Sz8LtK5UkXJHeWwdtbD4k-bnqtgen_A901payq4D4wkSL-P","name":"ESTSAUTHPER
SISTENT","httpOnly":true},{"path":"/","domain":"login.microsoftonline.com","expirationDate":1689951394,"value":"CAgABAAIAAAD--DLA3VO7
QrddgJg7WevrAgDs_wQA9P_En8yi4yHKMk_CSy2kcACCNEVWaNhld-fUAWFdNYyN5zuVm8pdQBqkIcjcnCk9vPQhacDObmplczszGhnk4o6V3DSgP8v3PDXbLnJwTkuQl6lg0
vOA-GzEBD-iHRY8V7rL_GafbP6CkPmgST4RPi1njsqD7N3tNULNGkhtXddSNDc6V5J76zO810jgNq_nMGZF0xooFD8H31D_qwK5GgLXxoTfToNrjMS0rSlneJXs1_FeTrn1CA
SSV97nDx-GB5eU-54Q","name":"SignInStateCookie","httpOnly":true},{"path":"/","domain":"login.microsoftonline.com","expirationDate":168
9951394,"value":"0.AU4A22TlbX0IWUike5T6K2izp1tEZUfGMrBJg-Ydk3ZSdspOAC0.AgABAAQAAAD--DLA3VO7QrddgJg7WevrAgDs_wQA9P8NHatOzr8eoH4wc7StgB
3hQAZlcD_ab6BIfatFR9FKLO442zIzQV3YMk1G4A_wenOa4Bbch4YhKg","name":"ESTSAUTH","httpOnly":true}]
```

The Cybersecurity Pathway

AHT INSURANCE
A BALDWIN RISK PARTNER

delcor®

grf CPAs & ADVISORS

Cybersecurity Pathway

What is your baseline?

- Identify risk to the achievement of your objectives
- Preform a risk assessment to help catalog your digital and physical assets.
  - This should include an internal and external scan depending on the network.
  - Frequently we find devices that clients believed were already decommissioned.
- What is the organization's "Crown Jewels"?
  - What systems are in place to protect those?

Cybersecurity Program

- Select a framework to benchmark against.
  - ISO 27001, NIST 800-53, PCI-DSS, etc…
- Develop policies and procedures to protect the organization's "Crown Jewels"
- Policies should have a purpose; don't need to be overly complicated
  - Don't leave it up to interpretation

PCI Security Standards Council®

Information Security Management ISO 27001 Certified

RECOVER IDENTIFY PROTECT DETECT RESPOND CYBERSECURITY FRAMEWORK VERSION 1.1

Does everyone know the risks?

- 97% of users can't recognize a phishing email.
  - Perform semi-annual cybersecurity trainings, more frequent the better.
  - Preform phishing simulations
- Send out bulletins about current events and what to look out for
- Ensure everyone knows your Information Security policy!

grf CPAs & ADVISORS

AHT INSURANCE
A BALDWIN RISK PARTNER

delcor

Are We Really Protected?

- Perform annual IT audits
  - Internal Threat Assessment, Third Party Risk Assessment, Access Reviews, Tabletop Exercises, Penetration Tests, Vendor Audit, Compliance Framework Audit.
  - IT departments and Managed Service Providers are amazing, but who is watching the watcher?
- IT is complex, many do not understand and do not verify

Common Misconceptions

"We're entirely cloud-based, so we don't have any risk, nor do we need a disaster recovery process"

- Even in a fully cloud-based environment, you can still be susceptible to malware, phishing attacks, and insider threats
- Cloud-based applications can create less visibility into network operations and result in "dark spots"
- Backup and recovery procedures are still required to mitigate data loss from cyber attacks, insider threats, physical damage
- If you are phished or your credentials are leaked, these cloud-based applications are still at risk

"We're small, so we have minimal risk and don't need cyber insurance"

- Hackers do reconnaissance and are likely to target smaller organizations because of limited resources
- It's not a matter of if, but when you will get hacked – don't get caught holding the bag
- Contact providers outside of your general business liability insurance provider – cheaper premiums

"Yes we have cybersecurity awareness training, we send out monthly eblasts and communicate top risks"

- This is better than nothing, but not adequate – no way to measure effectiveness and/or end user comprehension
- Follow up "it's too expensive for an org. our size." No it's not – platforms offer costs as low as $2/user
  - Knowb4, Hook Security, Barracuda

Potential Management Letter Comments

Our IT and Risk Management Questionnaire reflects latest PPC updates:

- Information Security Policies
  - Lack of policies and procedures documenting Information Technology General Controls (ITGCs)
- Segregation of Duties
  - One individual has System Administrator access to multiple platforms and/or is the sole System Administrator for a platform
- Review of System Administrator Activity
  - No procedures in place to monitor activity of System Administrators
- Access Management
  - Inappropriate assignment and/or monitoring of user access rights
- Third-Party Risk Management
  - No process for assessing risk related to third parties, specifically those with access to system, data, PII, financials, etc.

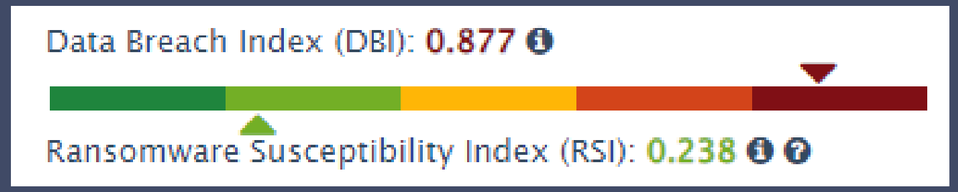
Technology That Helps

AHT INSURANCE
A BALDWIN RISK PARTNER

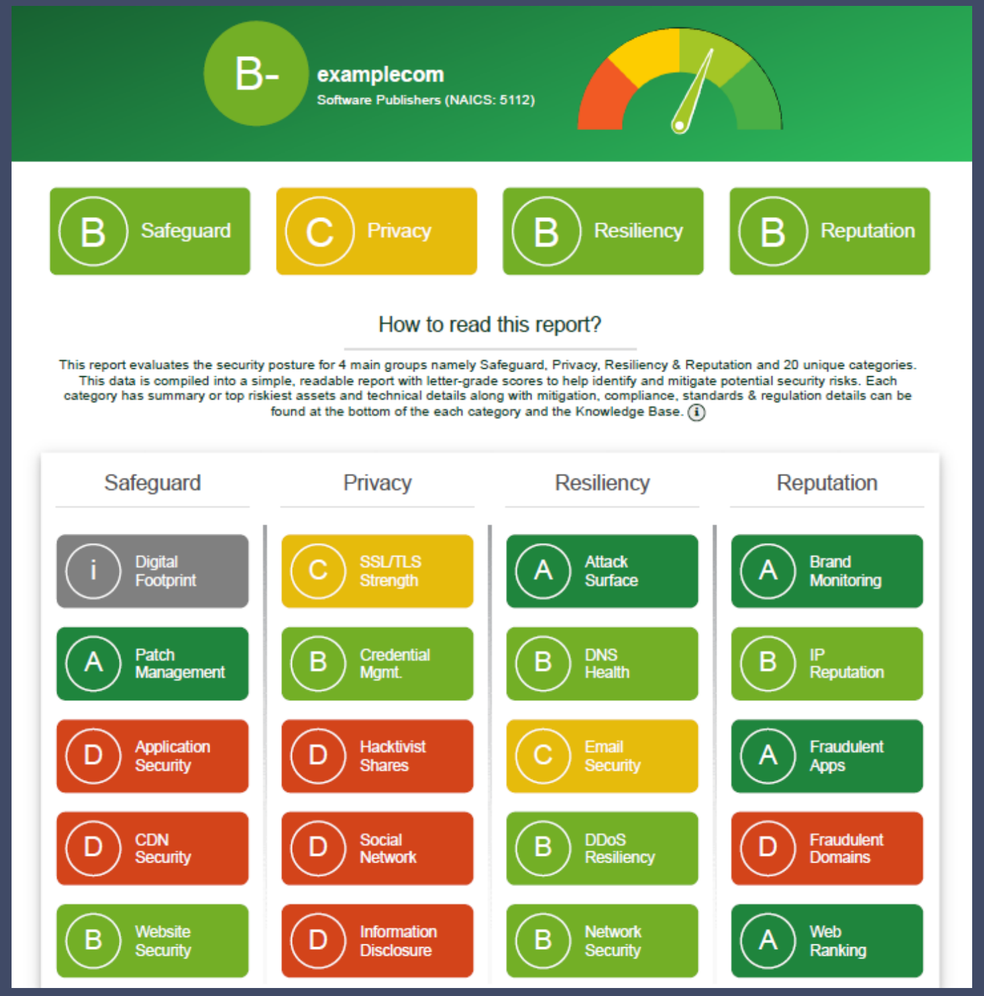
delcor

grf CPAs & ADVISORS

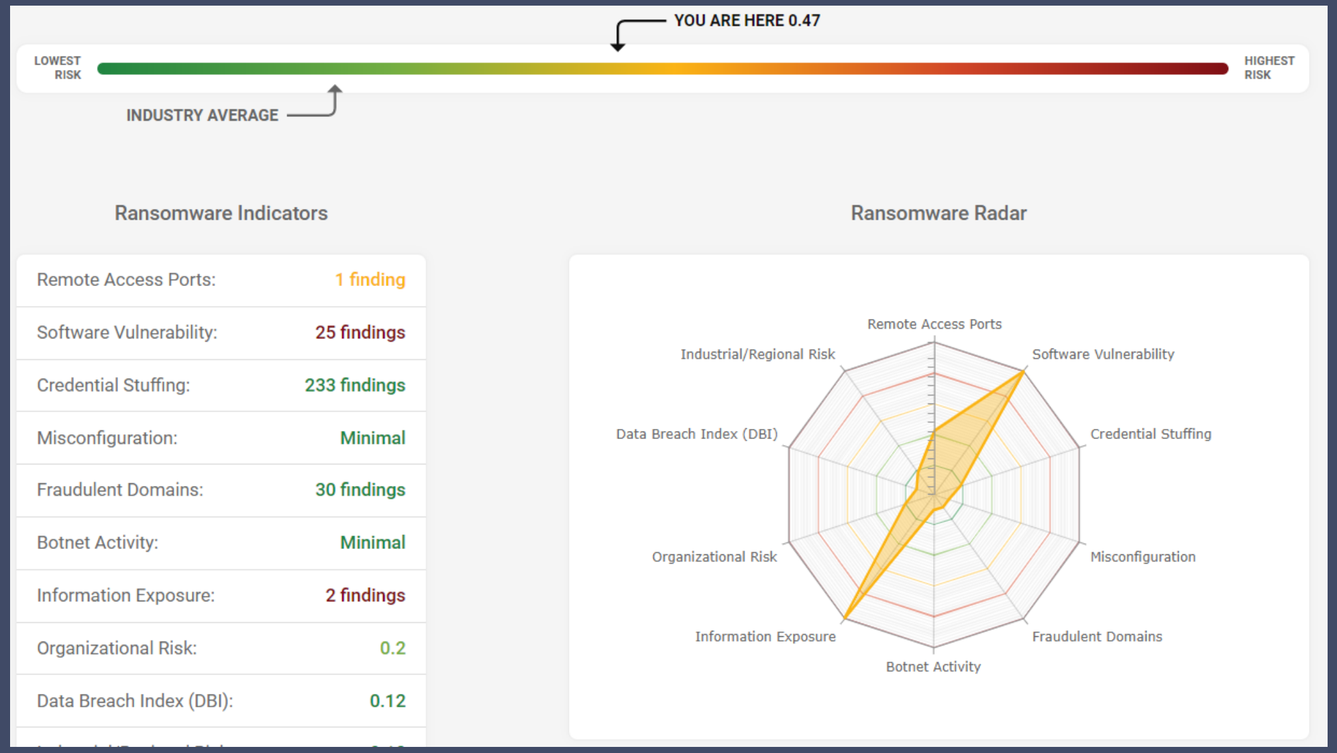
Embracing Technology



https://www.grfcpa.com/cyber-security-scorecard



Embracing Technology



Ransomware Indicators

Remote Access Ports:	1 finding
Software Vulnerability:	25 findings
Credential Stuffing:	233 findings
Misconfiguration:	Minimal
Fraudulent Domains:	30 findings
Botnet Activity:	Minimal
Information Exposure:	2 findings
Organizational Risk:	0.2
Data Breach Index (DBI):	0.12

Ransomware Radar

FAIR Analysis

FAIR Analysis Cont...

AI Gone Rogue

AI should be the start not the end result

CCPA Drafted Regulations

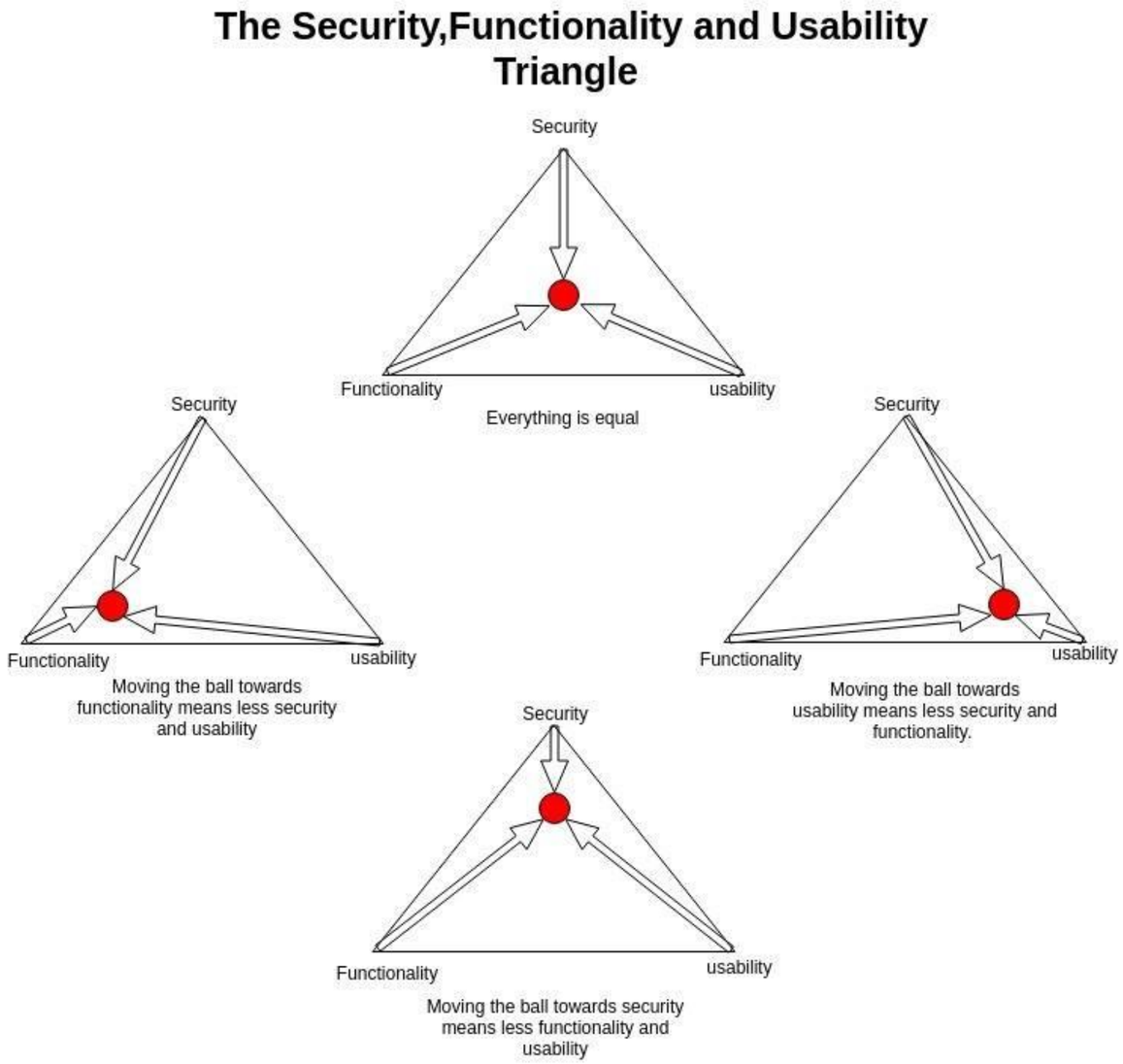
Requiring annual independent, detailed cybersecurity audits for businesses whose use and processing of consumer data meets a threshold for presenting a "significant risk" to consumer security

The auditor is specifically required to report issues regarding the cybersecurity audit directly to the business's board of directors or governing body, as opposed to reporting issues to business management with direct responsibility for the business's cybersecurity program

https://www.jdsupra.com/legalnews/cppa-posts-draft-rules-on-cybersecurity-5762307/

IT System Triangle

IT System Triangle



Basic Cybersecurity

AHT INSURANCE
A BALDWIN RISK PARTNER

delcor

grf CPAs & ADVISORS

Reactionary CyberSecurity

- Multi-Factor Authentication (MFA)
- Antivirus (AV)
- Backups
- Mobile Device Management
- User Awareness Training

Advanced Cybersecurity

AHT INSURANCE
A BALDWIN RISK PARTNER

delcor

grf CPAs & ADVISORS

Proactive CyberSecurity

- Web Application Firewall (WAF)
  - Protection for Members' Information
  - Protection from Targeted Attacks
- IT Policy and Procedures
  - Disaster Recovery (DR)
  - Incident Response (IR)
  - Recovery Metrics (i.e., RPO/RTO)
- Security Operations Center (SOC)

Zero Trust Architecture

AHT INSURANCE
A BALDWIN RISK PARTNER

delcor

grf CPAs & ADVISORS

Zero Trust Model

- Zero Trust is a conceptual process as opposed to a guided network architecture.
- Zero Trust assumes no “safe network” or “approved location” and goes hand in hand with Rights of Least Privilege.
- True Zero Trust is highly restrictive.
  - Understanding data value is key to implementing Zero Trust successfully.

IT Trade-Offs

AHT INSURANCE
A BALDWIN RISK PARTNER

delcor

grf CPAs & ADVISORS

IT Trade-Offs

- Vendor management is always easier than security management.
- Never spend more to protect something than it’s worth.
- Advancing from reactive to proactive doesn’t have to be a solo journey.

Cyber Liability and Ransomware

AHT INSURANCE
A BALDWIN RISK PARTNER

delcor

grf CPAs & ADVISORS

Common Claims Examples/ Types of Incidents

- Ransomware / Cyber Extortion Actions
- Phishing / Social Engineering (Financial and/or Data) Attempts and Successes
- Actual, attempted, and/or suspected intrusion and/or breach of CSBS's network
  - This extends to and includes 3rd party contracted services/managed networks
- Lost/Stolen laptop or mobile device
- Paper record breaches where privileged information is denoted

Cyber Liability Coverages – The Basics

Third-Party Coverages

- Network Security & Privacy Liability e.g. lawsuits, arbitration/mediation actions, etc.
- Regulatory Defense Expenses & Fines including PCI-DSS Fines & Penalties

First-Party Coverages

- Computer Forensics & Security Breach Remediation
- Privacy Breach Response Costs e.g. notification, legal, credit monitoring, etc.
- Crisis Management Event Expenses including Public Relations Expenses
- Cyber Extortion / Ransomware
- Cyber Crime (Social Engineering & Telecommunications Fraud)
- Business Interruption & Contingent or Dependent Business Interruption (Revenue Loss Coverage from a Cyber Claim)
- Data Restoration

Cyber Event Best Practices

1

Report under the Cyber Liability policy & Trigger Internal Crisis Management Team Procedures

Reporting should occur regardless of whether you think it will fall under the policy deductible.

2

Crisis Management Group Activation

Control knowledge access of the event and trigger protocols based on internal Crisis Management team and advise from Cyber Breach Response Team

3

Attorney/Client Privilege

Reporting to insurance carrier will trigger legal representation first and allow counsel to consult in a legally privileged manner in conjunction with the outsourced breach investigator

4

Consider Current Environment and Backups to be "At Risk" and Exposed

Work to verify overall scope of compromise and which systems/areas remain "safe".

Cyber Event Best Practices

5

Internal Communication – Determine Safest Method Given Scope of Compromise

Based on scope of the breach, should non-corporate phone and email correspondence be considered? Is phone VOIP safe?

6

Don't Negotiate or Engage before Specialists are Engaged for Ransomware

Triggering the policy will allow for the utilization of advice and guidance from team of cyber breach experts to delineate best response & approach to extortionists.

7

Reporting to Authorities

Work with insurance carrier Cyber Breach Team on required reporting to appropriate authorities e.g. FBI, regulatory bodies, etc.

8

After Action Review

What are the lessons learned and what steps can be taken to prevent similar events in the future?

Disclaimer

This webinar is not intended as, and should not be taken as, financial, tax, accounting, legal, consulting or any other type of advice. While we use reasonable efforts to furnish accurate and up-to-date information, we do not warrant that any information contained in or made available in this webinar is accurate, complete, reliable, current or error-free. We assume no liability or responsibility for any errors or omissions in the content of this webinar.

The use of the information provided in this webinar does not establish any contractual or other form of client engagement between GRF CPAs & Advisors and the reader or user. Any U.S. federal tax advice contained in this webinar is not intended to be used for the purpose of avoiding penalties under U.S. federal tax law. Readers and users of this webinar information are advised not to act upon this information without seeking the service of a professional accountant.