
grf
CPAs & ADVISORS
Stay Ahead of Evolving Risks
3-Part Risk Management Webinar Series
Board Engagement
SEP 21
11 AM - 12 PM
Cybersecurity
OCT 11
11 AM - 12 PM
Fraud Mitigation
NOV 16
11 AM - 12 PM
Please note: You do not need to attend all webinars in the series, each session can stand alone.

Your Organizations Guide to Cybersecurity

CPAs & ADVISORS

Melissa Musser,
CPA, CITP, CISA
Partner

Ricardo Trujillo,
CPA, CITP, CISA
Partner

Mac Lillard,
CPA, CFE, CISA,
CRISC, CITP
Manager

Darren Hulem,
CISA, Security+, CEH
Supervisor

GRF CPAs & Advisors

Personal Service With Powerful Solutions

Since 1981

600+ nonprofits

2022 Firms to Watch — accountingTODAY

2022 Regional Leaders — accountingTODAY

INSIDE PUBLIC ACCOUNTING TOP 200 FIRMS 2022

- Washington Business Journal's
  Top 25 Accounting Firms
- Accounting Today's
  Top Firms in the Capital Region for 2022

Housekeeping

Additional Information

Learning Objective To provide attendees with a better understanding of how to implement cybersecurity measures at your organization.	**Instructional Delivery Methods** Group Internet-based
Recommended CPE 1.0 CPE Credit	**Recommended Fields of Study** Risk Management
Prerequisites None required	**Advance Preparation** None
Program Level Basic	**Course Registration Requirements** None
Refund Policy No fee is required to participate in this session.	**Cancellation Policy** In the event that the presentation is cancelled or rescheduled, participants will be contacted immediately with details.
Complaint Resolution Policy GRF CPAs & Advisors is committed to our participants' 100% satisfaction and will make every reasonable effort to resolve complaints as quickly as possible. Please contact *kdavis@grfcpa.com* with any concerns.	
Disclaimer This webinar is not intended as, and should not be taken as, financial, tax, accounting, legal, consulting or any other type of advice. Readers and users of this webinar information are advised not to act upon this information without seeking the service of a professional accountant.	

Presenters

Meet the Instructors

Melissa Musser,

CPA, CITP, CISA

Partner

Ricardo Trujillo,

CPA, CITP, CISA

Partner

Mac Lillard,

CPA, CFE, CISA, CRISC, CITP

Senior Manager

Darren Hulem,

CISA, Security+, CEH

Supervisor

grf CPAs & ADVISORS

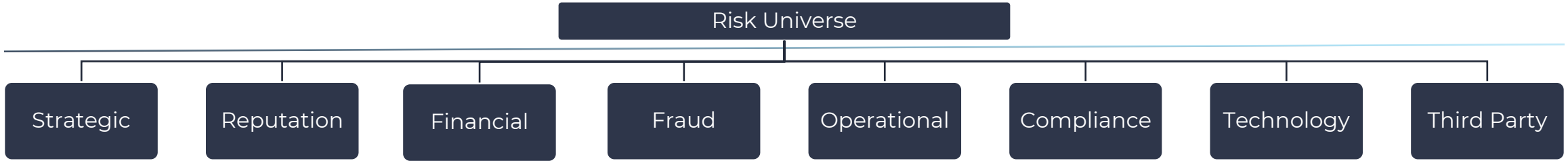
Agenda

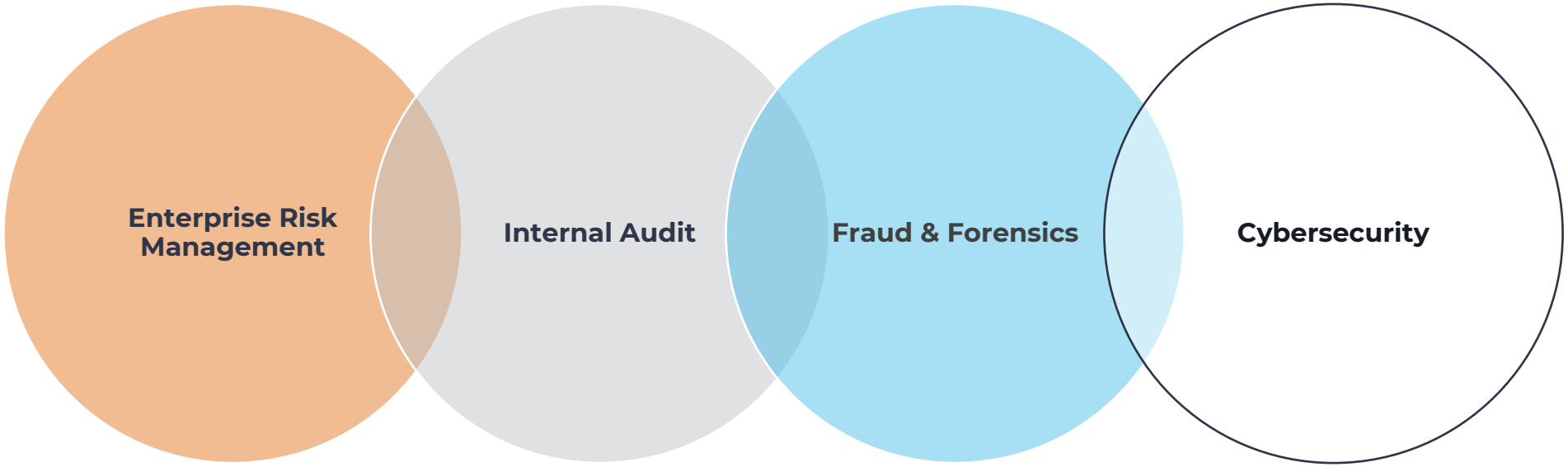
- Background and Introductions
- Current Landscape
- Monitoring your online reputation (What Can Google See)
- Reputation as a part of the Cybersecurity Pathway
- Closing Remarks and Contact Information
- Q&A

Where We Have Been

GRF has performed audits in over 100 different countries

Risk Advisory Tailored Solutions





GRF Cyber Solutions

Strategy

- Compliance framework benchmarking
- Policy and procedure development
- Data privacy and protection
- Virtual CISO
- Third party risk management
- IT strategy assessment
- IT mentoring

Security

- Cybersecurity audit
- Cyber risk assessment and scorecard
- Internal threat assessment
- Cyber training
- Identity and access management

Resiliency

- Incident response planning
- Disaster recovery planning
- Business continuity planning
- Tabletop exercises
- Penetration testing
- Data loss prevention

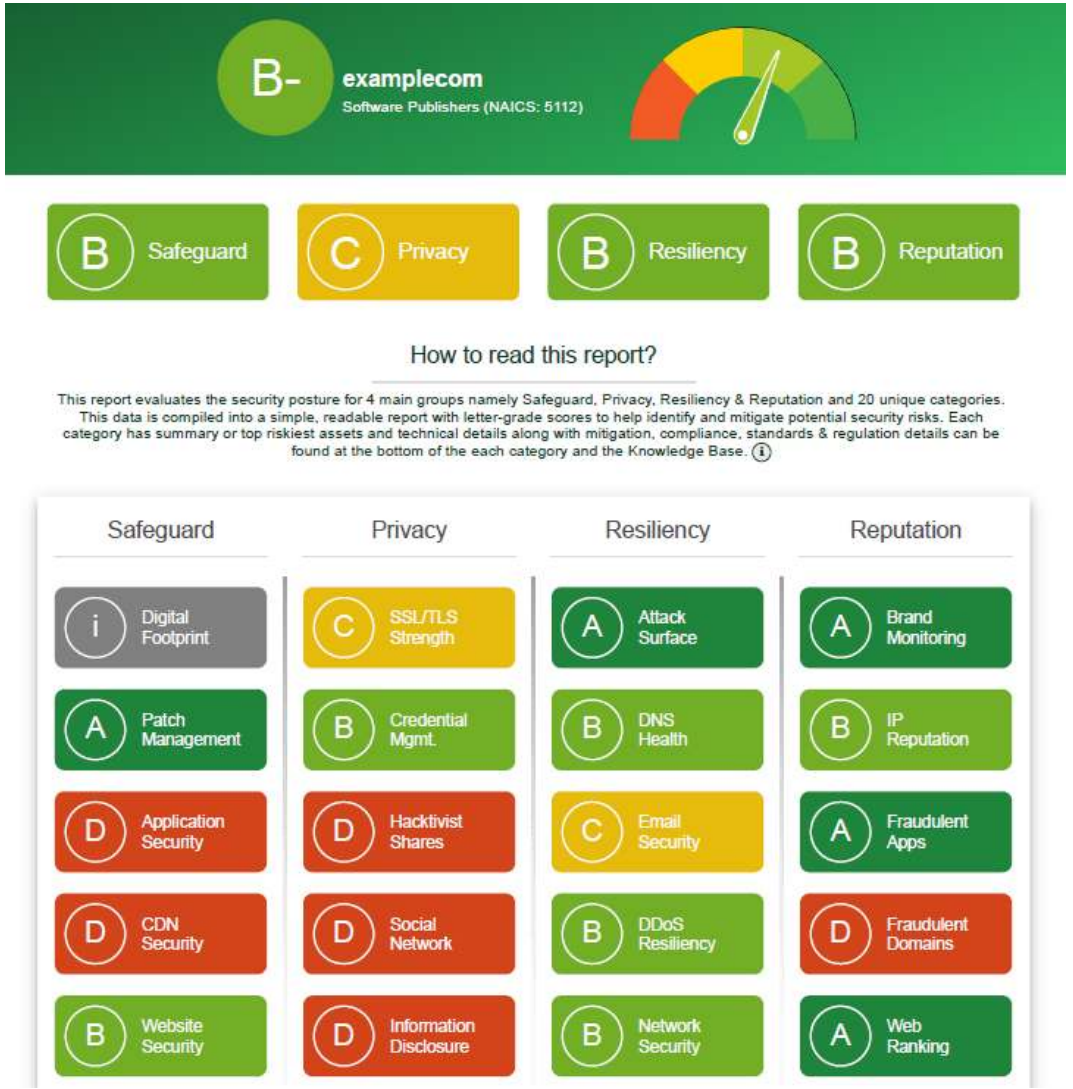
Current Landscape

Current Landscape

- Each year more goes from physical to digital
- Enhanced Reputation Risk

What Can Google See?

What can “Google” see?



Domains 81 | IP 1358 | Subdomains 355 | Dns Records 99 | Services 134 | Social Media 9 | Asn 60 | E-Mails ! | Geo Map | Company Information

Digital Footprint

A digital footprint is the record or trail left by the things you do online. How can you design a defense if you don't know what to defend?

Examples:

Different programs within the organization spin up their own websites without the IT department's knowledge

Client moved 100% to the cloud but found the old on-premise server was never decommissioned.

Polling Question #1

I feel my organization is safe with just traditional MFA, such as Microsoft/Google Authenticator, Duo, RSA, etc…

A. Yes

B. No

Patch Management

Service(s)	Total CVSS Score	# of Vuln(s)
php/7.4.1 nginx/1.19.2	81.2	12
windows server 2012 r2	53.6	8
windows server 2016	16.5	3

Service Version:

windows server 2012 r2
cpe:2.3:o:microsoft:windows_server:2012:r2:*:*:*:*:*:*

CVE-2022-26904 7.0

Description:

Windows User Profile Service Elevation of Privilege Vulnerability. **More about CVE-2022-26904**

References:

https://nvd.nist.gov/vuln/detail/CVE-2022-26904
https://capec.mitre.org/data/definitions/26.html
https://capec.mitre.org/data/definitions/29.html

EXPLOIT DATABASE

Verified Has App

Show 15

Date	D	A	V	Title
2022-04-26	⬇		✕	GitLab 14.9 - Stored Cross-Site Scripting (XSS)
2022-04-26	⬇		✕	Gitlab 14.9 - Authentication Bypass
2022-04-19	⬇		✕	EaseUS Data Recovery - 'ensserver.exe' Unquoted Service Path
2022-04-19	⬇		✕	PTPublisher v2.3.4 - Unquoted Service Path

Hacktivist Shares

- What is a hacktivist?
- What can be found in a hacktivist share?
- What is the risk of this information being leaked?

Information Disclosure

Data Breach Index	Do not Track	How do we collect your data
What data do we collect	Data Rights	Cookies Policy (How do we use and manage)
Changes to the privacy policy	Children's Online Privacy Protection	Privacy policy violations

Network Security

Publicly Accessible Critical Ports	Publicly Visible Remote Administration Ports	Anonymous FTP Site
• SMB (445), SQL (1433)	• Telnet, RDP, VNC. SNMP	• Ports (20 and 21)

Email / Username	Leaked Info	Password Type	Severity
[redacted]	****	PLAIN	Critical CWSS: 8
[redacted]	1e****	HASH	Critical CWSS: 8

Credential Management

- What should organization email addresses be used for?
- Password Policy
- Is MFA enabled?

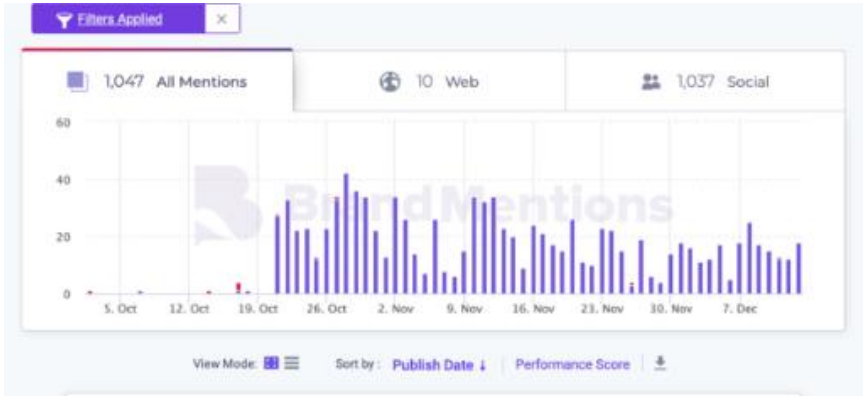
Vendor reliability	Child safety	Trustworthiness	Privacy
60%	n/a	60%	60%
Good		Good	Good

Brand Monitoring

- Web of Trust (WOT) Crowdsourced Web Safety
- Website optimization and Quality
- Social Profiles
- Domain Safety

Brand Monitoring Continued…

- Social Media Engagement
  - WFA – 40% of customers don't trust traditional advertising, rely on thoughts and experiences shared by peers.
- Understanding Sentiment
- Two-way communication
- Google Alerts, Brand24, Hootsuite, Brandmentions and BuzzSumo.

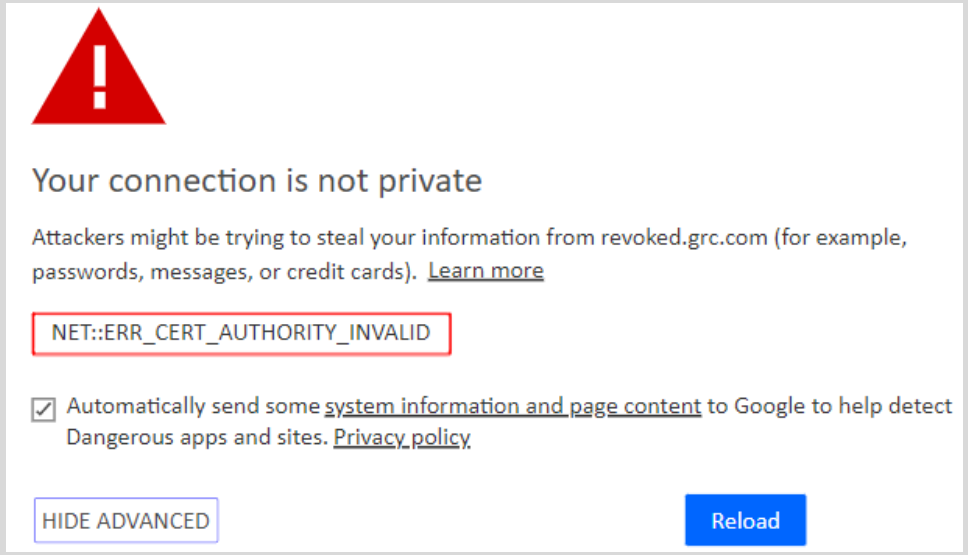


CPAs & ADVISORS

WFA – World Federation of Advertisers

SSL/TLS Strength

- SSL – Secure Socket Layer
- TLS – Transport Layer Security
- TLS 1.0 replaced SSLv3 but some use the terms interchangeably
- What to look out for:
  - Invalid, Expired, Self-Signed SSLs
  - POODLE, DROWN, BEAST attacks
  - Up to date CBC-Mode Ciphers



Fraudulent Domains

Whois Record (last updated on 2022-05-11)

```
Domain Name: facebook.com
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: https://www.registrarsafe.com
        http://www.registrarsafe.com
Updated Date: 2022-01-26T16:45:06+00:00
        2022-01-26
Creation Date: 1997-03-29T05:00:00+00:00
        1997-03-29
Registrar Registration Expiration Date: 2031-03-30T04:00:00+00:00
        2031-03-30
Registrar: RegistrarSafe, LLC
Sponsoring Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: 16503087004
```

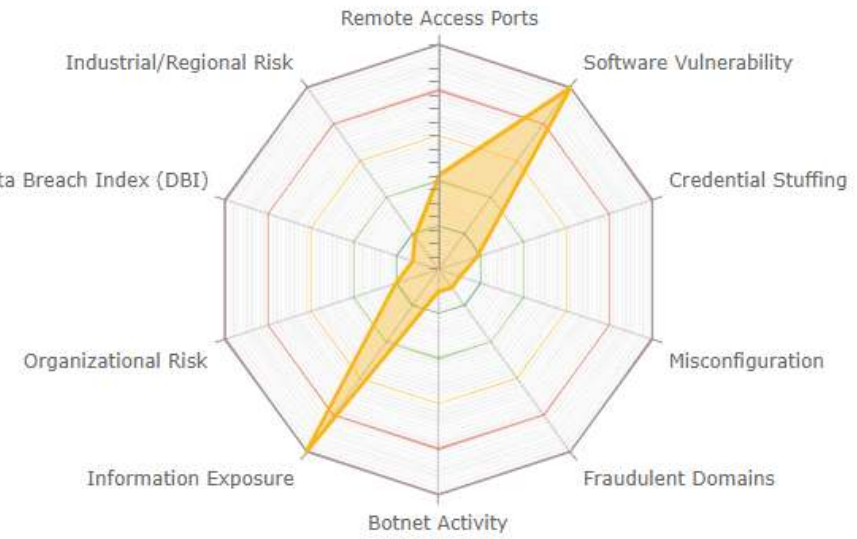
- What is typo squatting?
- Who owns the domain? Lookup.icann.org or whois.sc
- Spoofed website mirroring client's website – lead to e-mail scamming and false vendor invoice payments.
- INGO's in Ukraine, more likely to be targeted

Ransomware Index & TPRM

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
Industrial/Regional Risk:	0.18

Ransomware Radar



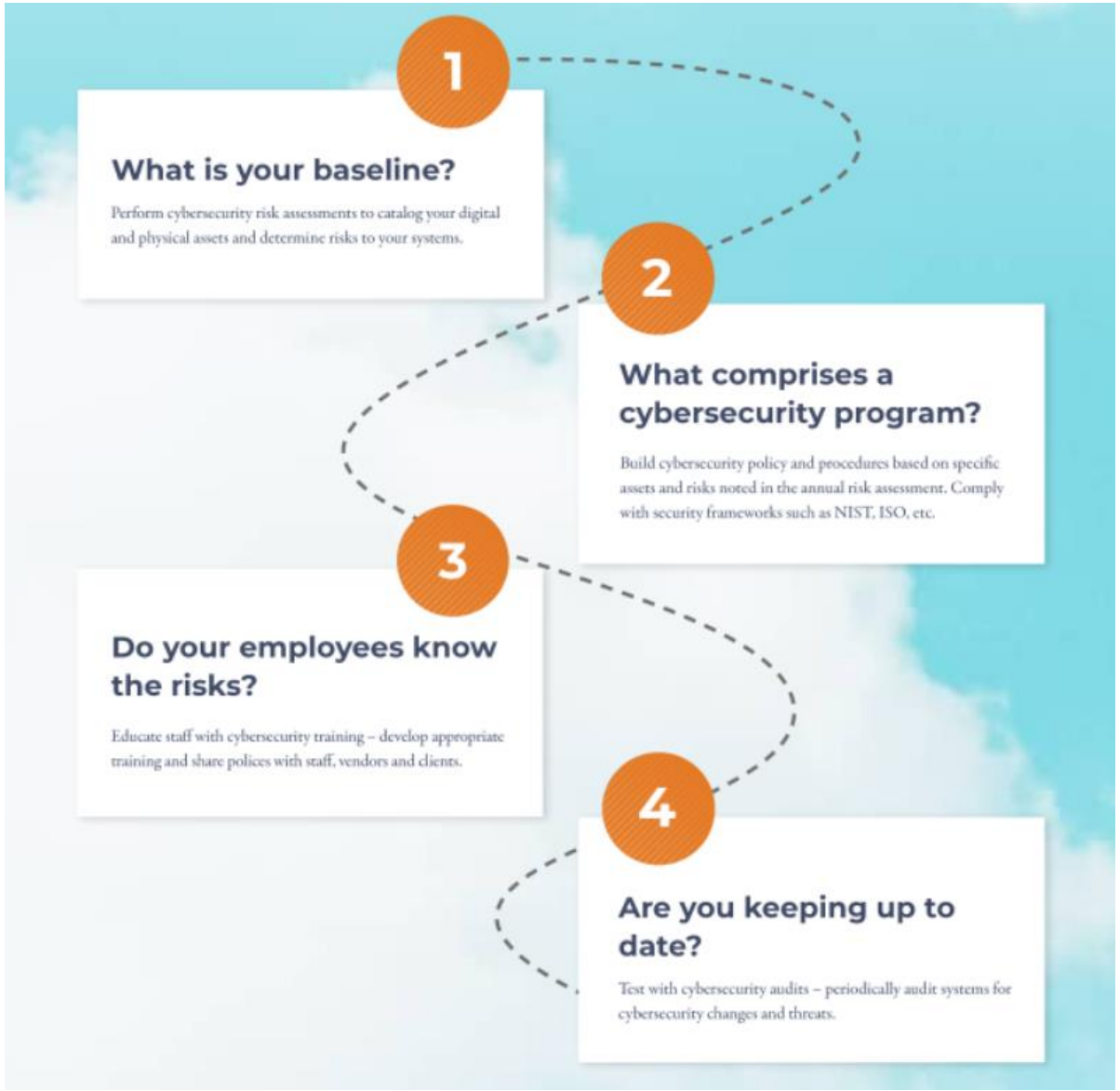
Polling Question #2

Does your organization follow an IT security framework?

A. *ISO*
B. *NIST*
C. *Other*
D. *No*
E. *Unsure*

Reputation as Part of a Cybersecurity Pathway

Cybersecurity Pathway



What is your baseline?

- 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

- Determine if your organization is required to comply with any IT security frameworks
  - 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

Does everyone know the risks?

- Preform semi-annual cybersecurity trainings
- Preform phishing simulations
- Send out bulletins about current events and what to look out for
  - New ransomware and attacks happening as a result of Russia in Ukraine.

Are we really protected?

- Preform annual IT audits
  - 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

Polling Question #3

Is cybersecurity a regular agenda item at Board meetings?

A. Yes

B. No

C. Unsure

Dysfunctional boards

1. Reluctance to discuss strategy or risk or both
2. A failure to refresh board composition resulting in stakeholder concerns
3. A failure to address succession planning
4. An inability to deal with disruptive behavior by a director
5. Board and committee structure that creates confusion or leaves issues uncovered

Source: https://boardmember.com/different-reasons-board-dysfunctional/

Executive Perspectives of Top Risks for 2022

Key Themes

Talent and Culture Concerns Dominate

+ Ongoing Pandemic Concerns

+ Cyber & Technology

Top Risks for 2022	
1	Pandemic-related government policies / regulation
2	Succession challenges; attract and retain top talent
3	Pandemic-related market conditions reduce demand
4	Digital technologies requiring new skills or significant efforts to upskill/reskill employees
5	Economic conditions constrain growth opportunities
6	Increasing labor costs impact profitability targets
7	Resistance to change operations / business model
8	Inability to utilize data analytics and "big data" to achieve market intelligence
9	Cyber threats
10	Shifts in social issues / diversity, equity, and inclusion

#14 – Third-party risks, including IT outsourcing
#15 – Legacy IT infrastructure, lack of digital expertise
#21 – Data privacy & security

NC STATE Poole College of Management
Enterprise Risk Management Initiative

Top Board Concerns - 2022

https://www.protiviti.com/US-en/insights/protiviti-top-risks-survey

Viewpoints Differ Re: "Significant Risks"

- Board members 0
- CEOs 13
- CFOs 1
- CTOs/CIOs 17

Who is correct?

Quick Takeaways

INFORMATION IS READILY AVAILABLE FOR ANYONE TO SEE ONLINE

DETERMINE YOUR ORGANIZATIONS BASELINE

CONTINUE TO DEVELOP YOUR CYBER PROGRAM

ENSURE EVERYONE KNOWS THE RISKS

TRUST BUT VERIFY

Explore GRF Resources

- Cybersecurity and Privacy Risk Services
- GRF Cybersecurity Scorecard & Risk Assessment Demonstration
- Cybersecurity Blog Series
- Subscribe to GRF Newsletters
- Read Our Whitepaper – Elements of Successful Cybersecurity

grf CPAs & ADVISORS

Questions?

Contact Us

CPAs & ADVISORS

www.grfcpa.com

Melissa Musser,
CPA, CITP, CISA

mmusser@grfcpa.com
301-951-9090

Ricardo Trujillo,
CPA, CITP, CISA

rtrujillo@grfcpa.com
301-951-9090

Mac Lillard,
CPA, CFE, CISA, CRISC, CITP

mlillard@grfcpa.com
301-951-9090

Darren Hulem,
CISA, Security+, CEH

dhulem@grfcpa.com
301-951-9090


grf
CPAs & ADVISORS
Stay Ahead of Evolving Risks
3-Part Risk Management Webinar Series
Board Engagement
SEP 21
11 AM - 12 PM
Cybersecurity
OCT 11
11 AM - 12 PM
Fraud Mitigation
NOV 16
11 AM - 12 PM
Please note: You do not need to attend all webinars in the series, each session can stand alone.

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.