



Reputation Risk as Part of your Cybersecurity Program

Melissa Musser,
CPA, CTP, CISA
Partner

Mac Lillard,
CPA, CFE, CISA,
CRISC, CTP
Senior Manager

Darren Hulem,
CISA, Security+, CEH
Supervisor



Agenda

Current Landscape

- Reputation as a part of the Cybersecurity Pathway
- Monitoring your online reputation (What Can “Google” See)
- Closing Remarks and Contact Information
- Engaging the Board and Other Stakeholders
- Q&A



Presenters

Meet the Instructors



Melissa Musser,

CPA, CITP, CISA

Partner



Mac Lillard,

CPA, CFE, CISA, CRISC, CITP

Senior Manager



Darren Hulem,

CISA, Security+, CEH

Supervisor



GRF CPAs & Advisors



Personal
Service With
Powerful
Solutions

Since 1981

Located in the Washington D.C. Metro Region
Serving clients throughout the United States and Internationally.

GRF Solutions

Traditional
Audit & Tax

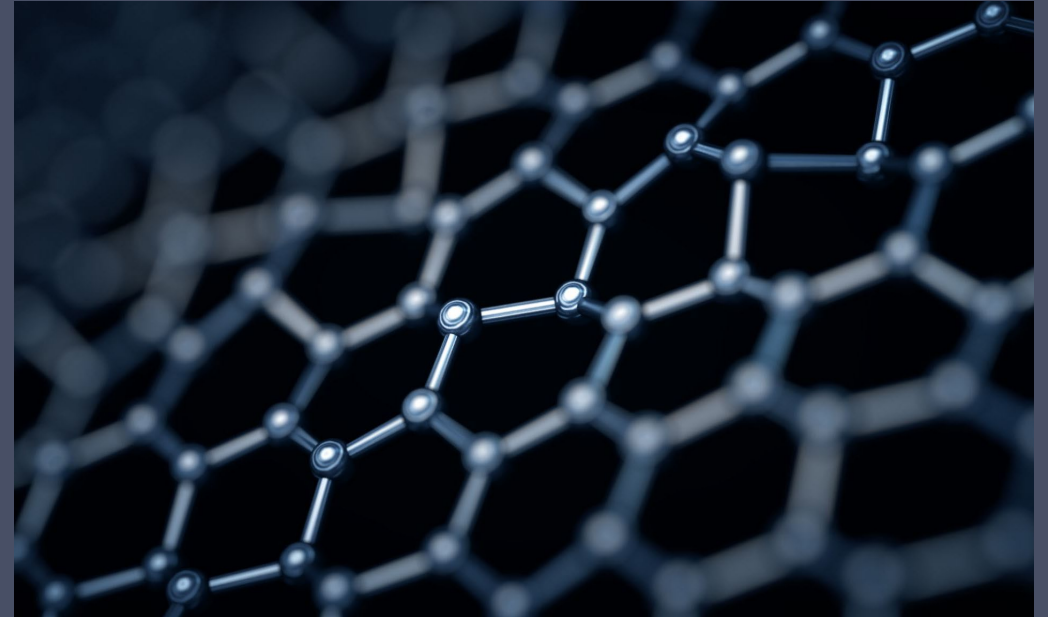
Outsourced
Accounting &
Technology

Enterprise
Risk
Management

Internal
Audit

Fraud &
Forensics

Cybersecurit
y



CPAs & ADVISORS



CPAs & ADVISORS



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

GRF Cyber Solutions

<https://www.grfcpa.com/accounting-services/cybersecurity-and-privacy-risk-solutions/>



Current Landscape

7



Current Landscape



Each year more goes from physical to digital



Enhanced Reputation Risk



Losing sight of the basics



Risks

- Cybersecurity, Information Security and Data Privacy
 - How is your organization protecting the network/systems/data?
- Business Continuity and Disaster Recovery Planning:
 - Minimize the negative effects of unforeseen risk events (i.e. cyber breach, fire, pandemic)
 - Disaster recovery planning is a component of business continuity planning that focuses on the restoration of systems to minimize downtime



Risks

- Third-Party Risk Management
 - What liability is posed to your organization through outside service providers?
 - Is your process for vetting, monitoring, and evaluation vendors adequate based on the level of risk associated with the relationship?
- Fraud Risk Management:
 - Are your employees properly trained to identify phishing emails, fraudulent domains, etc.?
 - Do you have banking controls such as Positive Pay implemented on online accounts?



What are malicious actors doing?

11



What malicious actors are doing

- The 5 stages of hacking
 - Reconnaissance
 - Scanning
 - Gaining Access
 - Maintaining Access
 - Clearing Tracks



What malicious actors are doing

- Ransomware
 - Crypto
 - Lockers
 - Scareware
 - Maze
 - WhisperGate and HermeticWiper



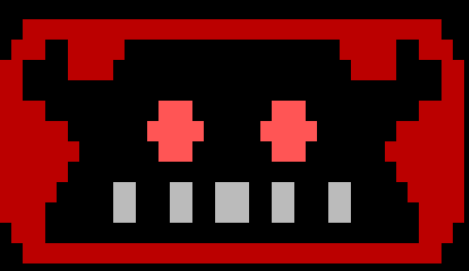
Polling Question #1

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

A. Yes

B. No





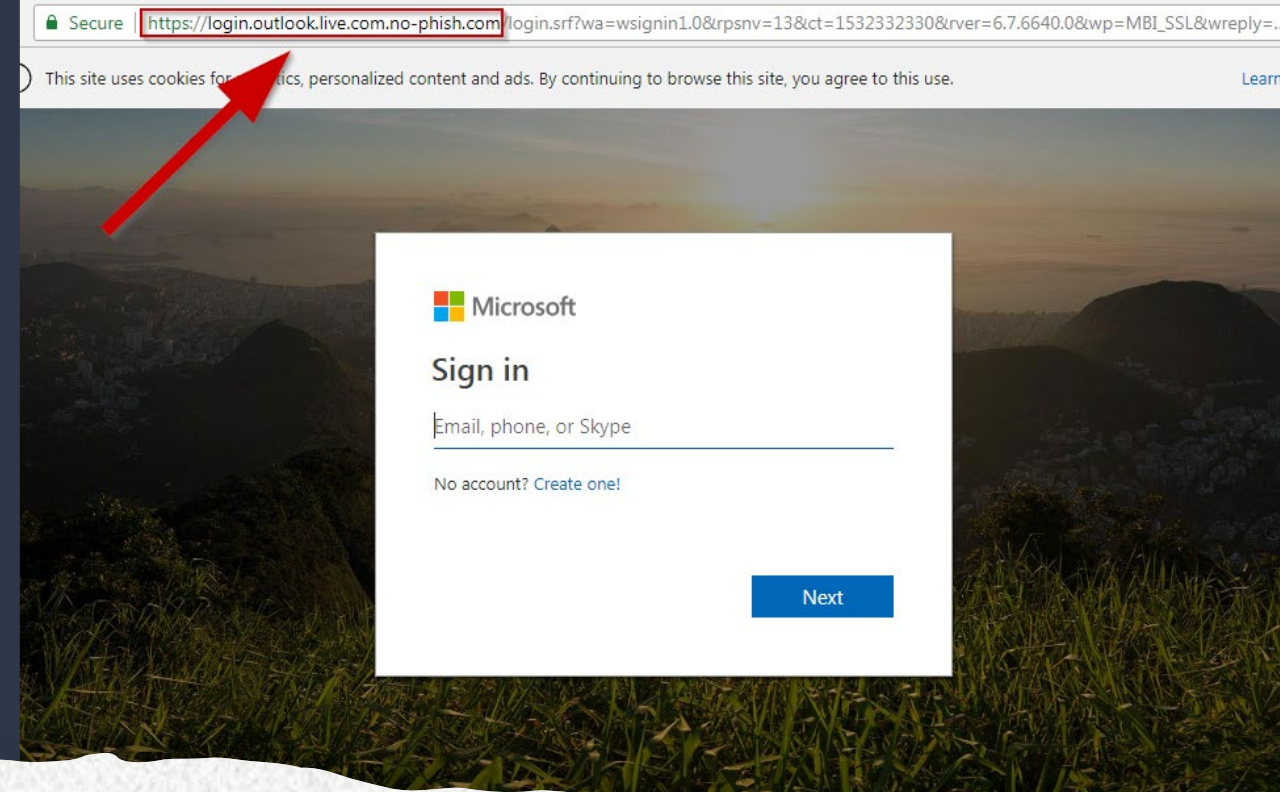
EvilginX

no nginx - pure evil

by Kuba Gretzky (@mrgretzky) version 2.3.1

```
[19:12:08] [inf] loading phishlets from: /usr/share/evilginx/phishlets/  
[19:12:08] [inf] redirect parameter set to: hb  
[19:12:08] [inf] verification parameter set to: zw  
[19:12:08] [inf] verification token set to: 20cd  
[19:12:08] [inf] unauthorized request redirection URL set to: https://www.youtube.com/watch?v=dQw4w9WgXcQ  
[19:12:09] [war] server domain not set! type: config domain <domain>  
[19:12:09] [war] server ip not set! type: config ip <ip_address>
```

phishlet	author	active	status	hostname
github	@audibleblink	disabled	available	
instagram	@prrrrinnee	disabled	available	
linkedin	@mrgretzky	disabled	available	
okta	@mikesiegel	disabled	available	
outlook	@mrgretzky	disabled	available	
reddit	@customsync	disabled	available	
twitter	@white_fi	disabled	available	
amazon	@customsync	disabled	available	
citrix	@424f424f	disabled	available	
facebook	@mrgretzky	disabled	available	
o365	@jamescullum	disabled	available	
protonmail	@jamescullum	disabled	available	
mobile	@white_fi	disabled	available	



What malicious actors are doing cont...

```

[09:28:46] [imp] [0] [google] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
67.0.3396.87 Safari/537.36 ([redacted])
[09:28:46] [inf] [0] [google] landing URL: https://accounts.docs.[redacted].com/signin/v2/identifier?hd=dUp4&ol=aHR0cHM6Ly93d3cuZ
C5jb20=
[09:29:40] [+++] [0] Username: [redacted]
[09:29:45] [+++] [0] Password: [redacted]
[09:29:57] [+++] [0] all authorization tokens intercepted!
[09:29:58] [imp] [0] redirecting to URL: https://www.dropbox.com
: sessions

```

id	phishlet	username	password	tokens	remote ip	time
1086	google	[redacted]	[redacted]	captured	[redacted]	2018-07-16 09:29

```
: sessions 1086
```

```

id : 1086
phishlet : google
username : [redacted]
password : [redacted]

```

What malicious actors are doing cont...

```

landing URL: https://accounts.docs.[redacted].com/signin/v2/identifier?hd=dUp4&ol=aHR0cHM6Ly93d3cuZC5jb20=
user-agent : Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
remote ip : [redacted]
create time : 2018-07-16 09:28
update time : 2018-07-16 09:29

```



```

[{"path": "/", "domain": "accounts.google.com", "expirationDate": 1563269413, "value": "1:SeA2lf_9K9cYes1sK-Zxf4IJYbFuExL7kzR7MhRKJymxHJibcsG
TNJ-EnkDGZ00kluJYWfU3leP-pKgmI5z0_g:ZYrZlHOEDfcAX0TT", "name": "GAPS"}, {"path": "/", "domain": "accounts.google.com", "expirationDate": 1563269413, "value": "PwaNHSJvu9q3BIuKdp-VGNWP6pa78vOk1AAkiC41dU8QVT27WFnHFUAdxeqkwqTJQzdcw.", "name": "LSID"}, {"path": "/", "domain": "google.com", "expirationDate": 1563269413, "value": "7aV8JVGVGF1dtyOx/AmWcSzaItWrT1JhsD", "name": "APISID"}, {"path": "/", "domain": "google.com", "expirationDate": 1563269413, "value": "7aV8JVGVGF1dtyOx/AmWcSzaItWrT1JhsD", "name": "APISID"}]

```



Reputation as Part of a Cybersecurity Pathway

17



Cybersecurity Pathway



What is your baseline?

- Identify risk to the achievement of your objectives
- Perform 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



Polling Question #2

Does your organization follow an IT security framework?

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



Ohio Data Protection Act

- The Ohio Data Protection Act ("Ohio DPA") provides a safe harbor against data breach lawsuits for businesses that implement and maintain cybersecurity programs that meet certain industry-recognized standards.
- “Reasonable Security” in today’s cybersecurity is following a cybersecurity framework
 - NIST Cybersecurity Framework, 800-53, 800-171
 - ISO 27001
 - CIS CSC (Also known previously as the SANs TOP 20)
 - SOC 2
 - HIPAA, FISMA, PCI-DSS



Does everyone know the risks?

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

[GRF Awareness Training https://www.grfcpa.com/wp-content/uploads/2022/10/GRF-Cybersecurity-Awareness-Training.pdf](https://www.grfcpa.com/wp-content/uploads/2022/10/GRF-Cybersecurity-Awareness-Training.pdf)



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



What Can Google See?

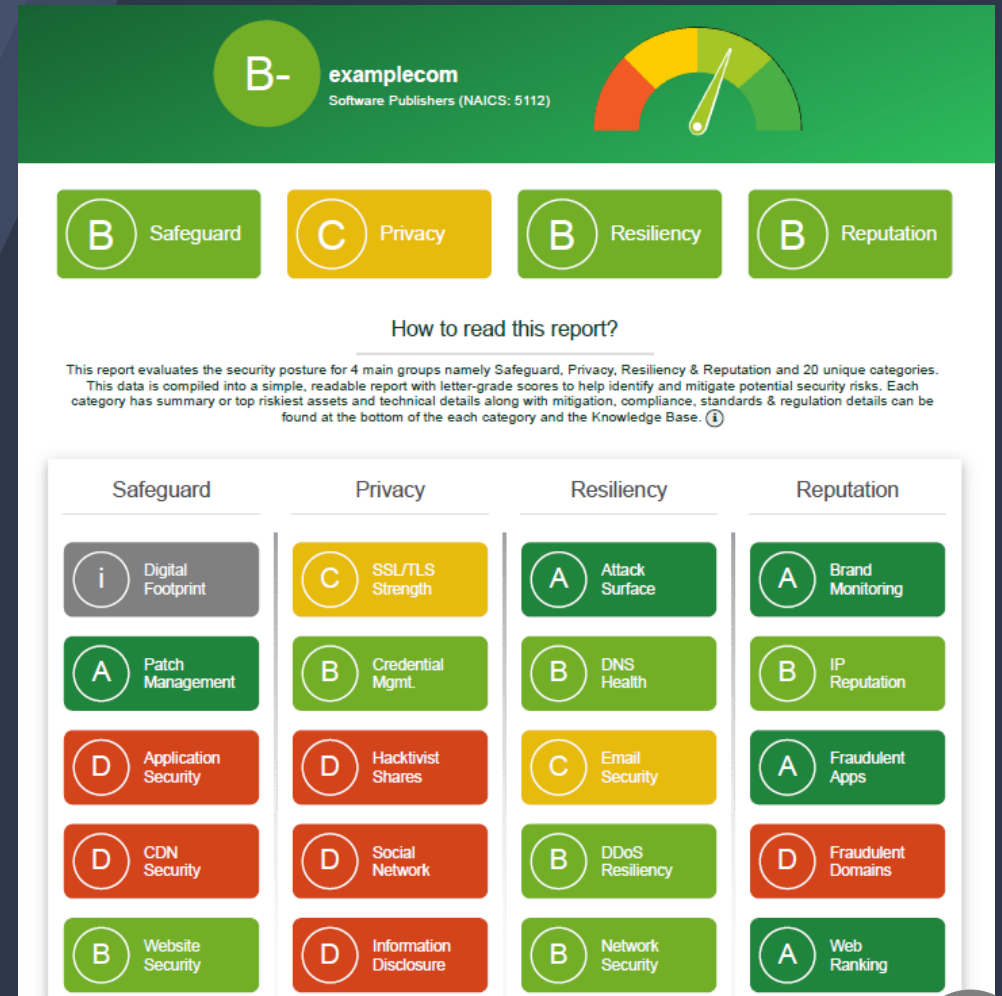
25



What can “Google” see?



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



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.



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>



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

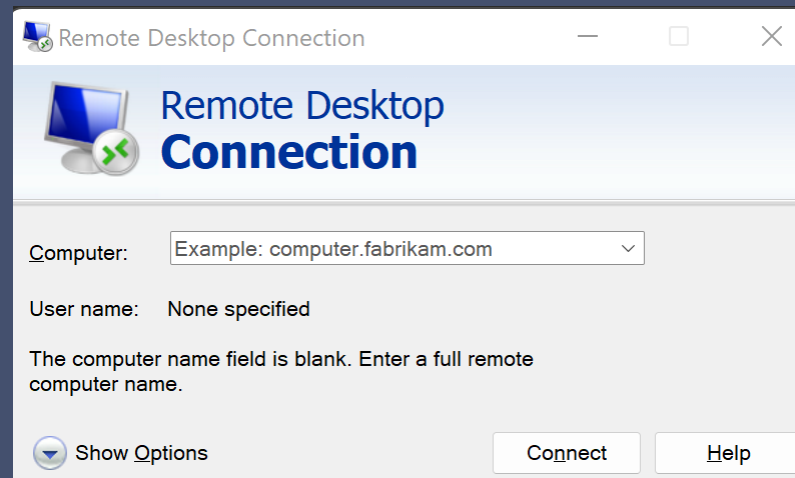
- SMB (445), SQL (1433)

Publicly Visible Remote Administration Ports

- Telnet, RDP, VNC.
SNMP

Anonymous FTP Site

- Ports (20 and 21)



	Email / Username	Leaked Info	Password Type	Severity
	rob.hendricks@kansaspa.com	****	PLAIN	<div style="background-color: #800000; color: white; padding: 2px 5px; display: inline-block;">Critical</div> <div style="background-color: #555; color: white; border-radius: 10px; padding: 2px 5px; display: inline-block;">CWSS: 8</div>
	rob.hendricks@kansaspa.com	1e****	HASH	<div style="background-color: #800000; color: white; padding: 2px 5px; display: inline-block;">Critical</div> <div style="background-color: #555; color: white; border-radius: 10px; padding: 2px 5px; display: inline-block;">CWSS: 8</div>

Credential Management

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



Polling Question #3

Does your organization provide cyber awareness training and/or phishing simulations?

- A. *Yes*
- B. *No*
- C. *Unsure*



Brand Monitoring Continued...

Social Media Engagement

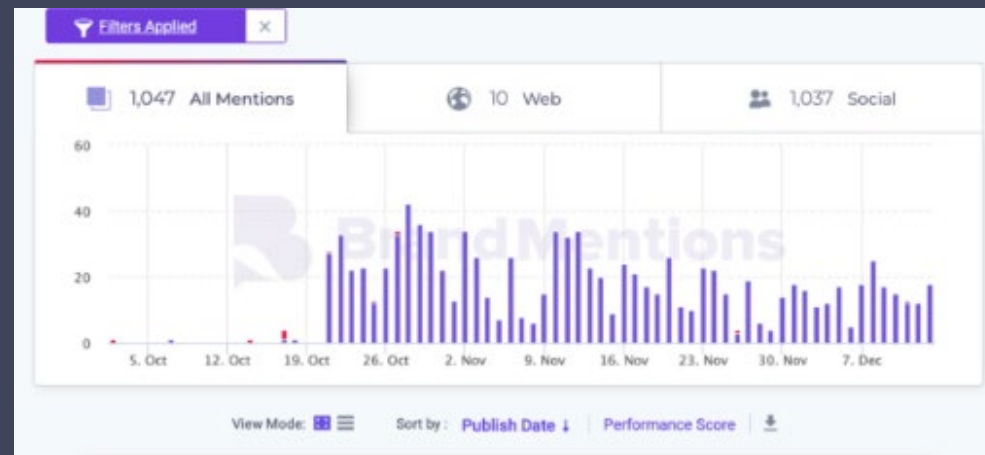
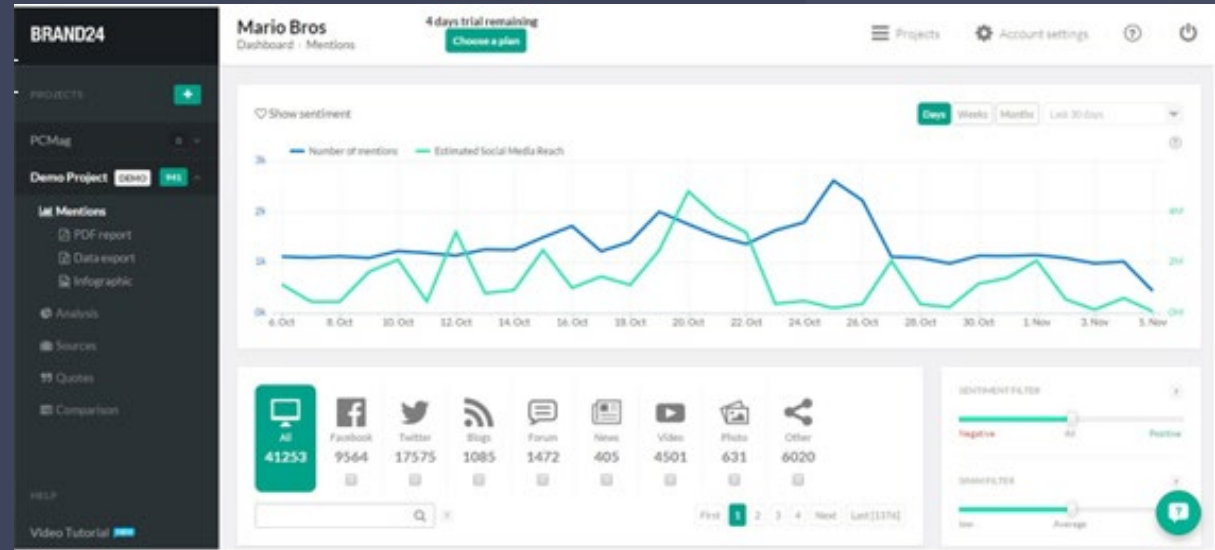
- WFA – 40% of customers don't trust traditional advertising, rely on thoughts and experiences shared by peers.

Understanding Sentiment

Two-way communication


Google Alerts, Brand24, Hootsuite, Brandmentions and BuzzSumo.

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



Your connection is not private

Attackers might be trying to steal your information from revoked.grc.com (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

Automatically send some system information and page content to Google to help detect Dangerous apps and sites. [Privacy policy](#)

HIDE ADVANCED Reload



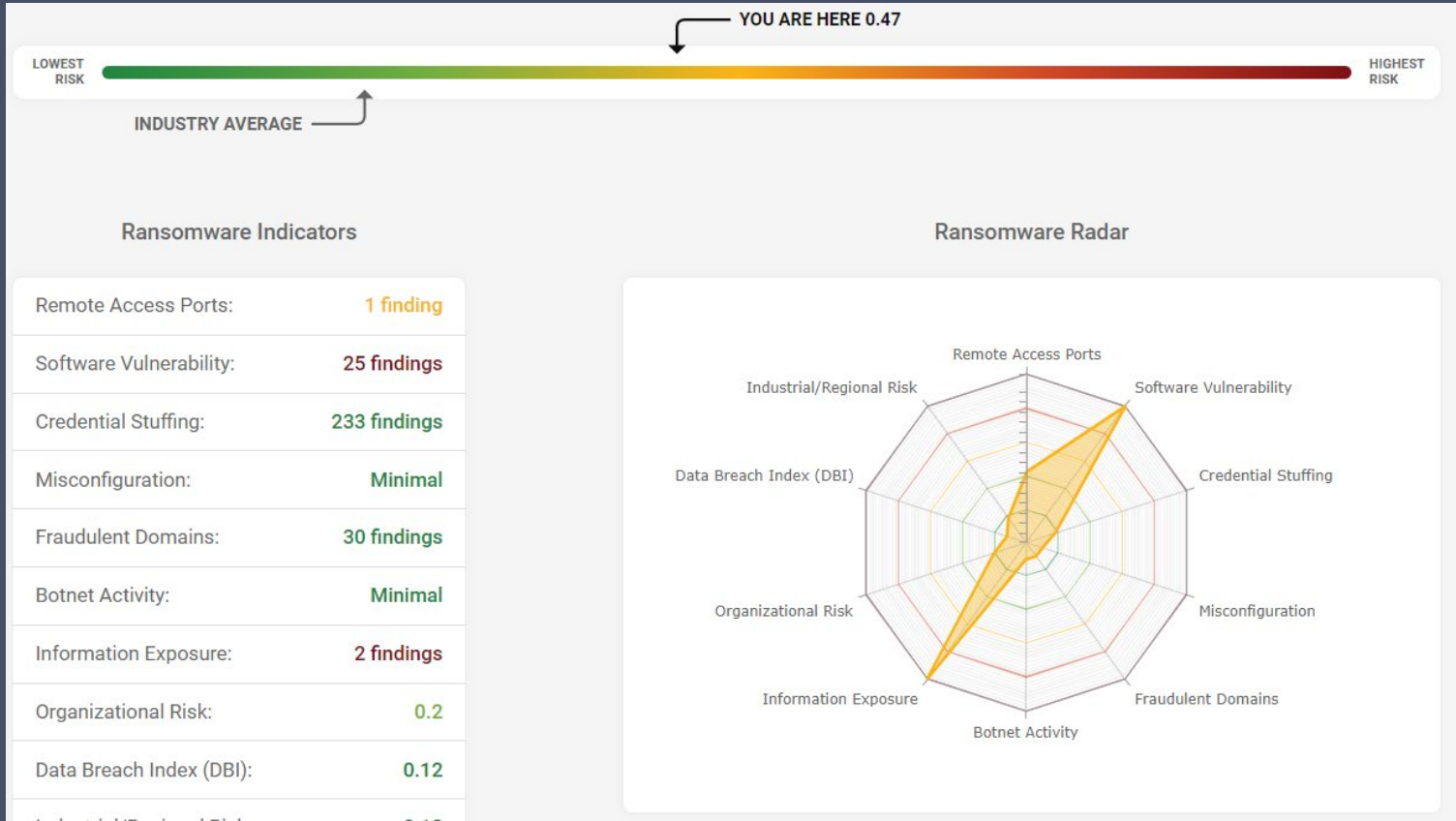
Fraudulent Domains

- 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.

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
```





Ransomware Index & TPRM

Engaging the Board and other Stakeholders

39



Polling Question #4

Is cybersecurity a regular agenda item at Board meetings?

- A. *Yes*
- B. *No*
- C. *Unsure*

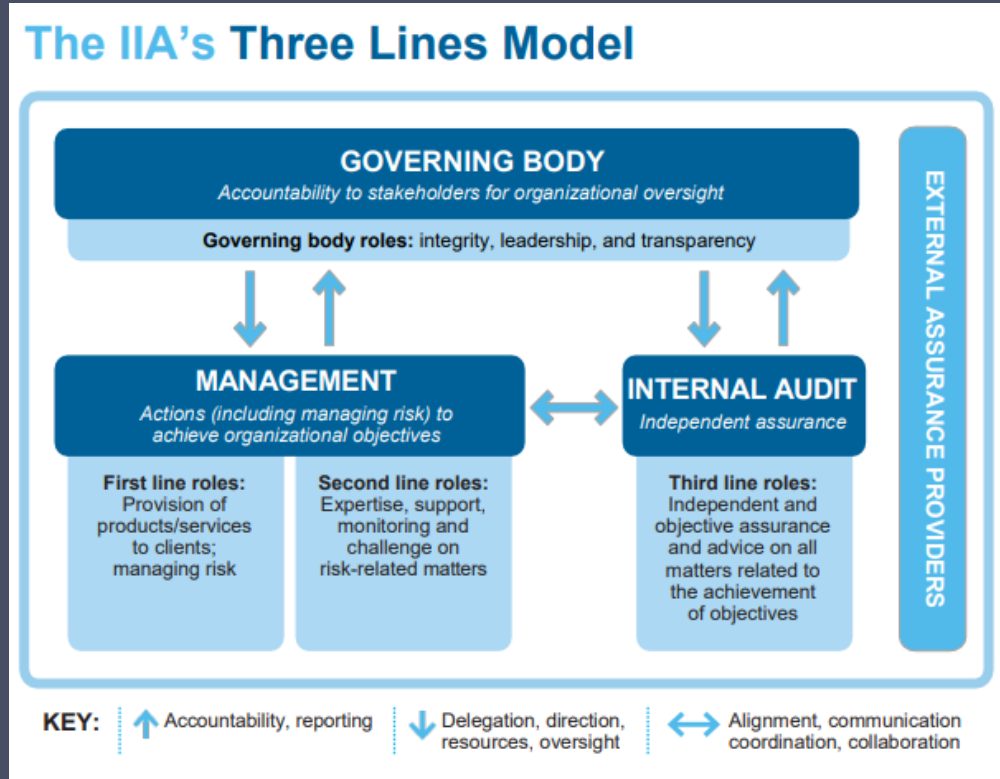
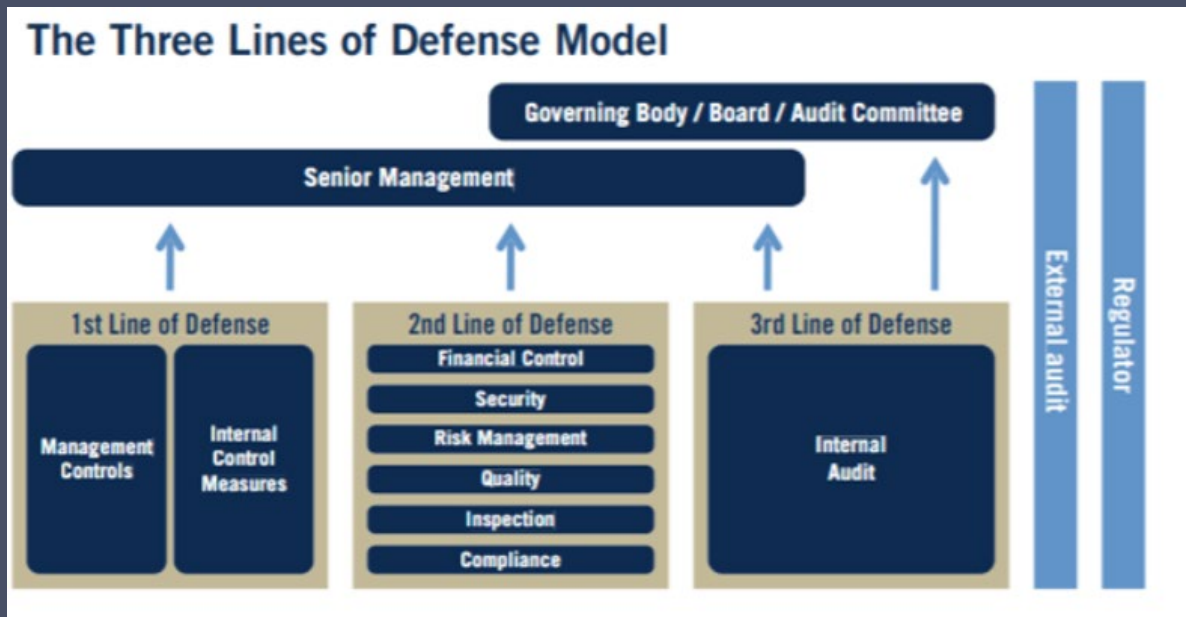


IIA's new "Three Lines Model" stresses collaboration

Previous Model



Updated Model



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/retrain 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

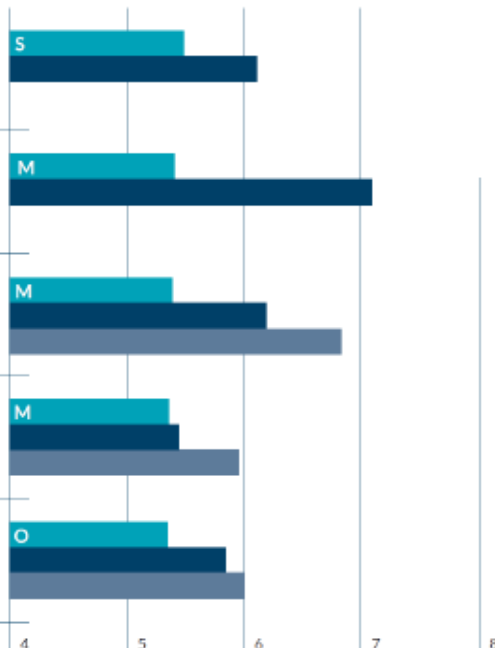
#14 – Third-party risks, including IT outsourcing
#15 – Legacy IT infrastructure, lack of digital expertise
#21 – Data privacy & security



Top Board Concerns - 2022

Board Members - 2022

Market conditions imposed by and in response to COVID-19 and emerging variants, including shifts in consumer behavior to digital channels, may continue to impact customer demand for our core products and services



Legend

M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue ■ 2022 ■ 2021 ■ 2020



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](#)



Questions

Contact Us



Melissa Musser,
CPA, CITP, CISA

mmusser@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



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.