



Thank you for joining us!

The presentation will begin shortly



accountingTODAY

2023 **Best Firms to Work For**

accountingTODAY

2023 **Firms to Watch**

accountingTODAY

2023 **Regional Leaders**





Cybersecurity: Is AI the Secret Weapon?

Melissa Musser,
CPA, CTP, CISA, CIA
Partner

Ricardo Trujillo,
CPA, CTP, CISA
Partner

Darren Hulem,
CISA, Security+, CEH
Manager



Presenters

Meet the Instructors



Melissa Musser,
CPA, CITP, CISA
Partner



Ricardo Trujillo,
CPA, CITP, CISA
Partner



Darren Hulem,
CISA, Security+, CEH
Manager



Housekeeping

Additional Information

Learning Objective To provide attendees with a road map cybersecurity and artificial intelligence.	Instructional Delivery Methods Group Internet-based
Recommended CPE 1.0 CPE Credit	Recommended Fields of Study Specialized Knowledge
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.	



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**

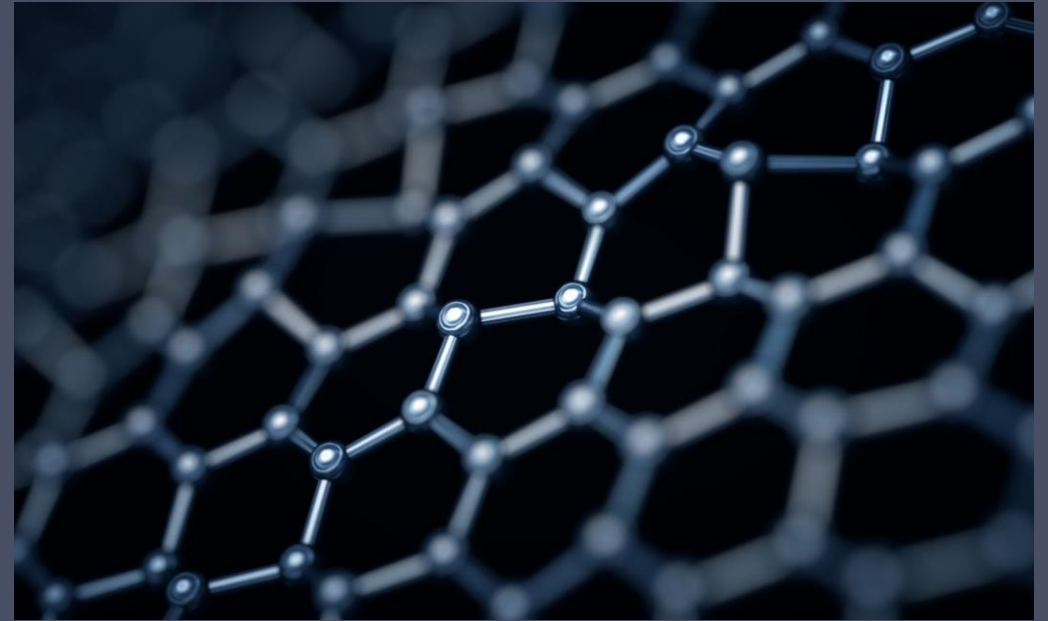
**Outsourced
Accounting &
Technology**

**Enterprise
Risk
Management**

**Internal
Audit**

**Fraud &
Forensics**

Cybersecurity



CPAs & ADVISORS



Agenda

Current Landscape

Understanding AI

How AI and other tech can help in the Cybersecurity Pathway

Culture

Closing Remarks and Contact Information

Q&A



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/>



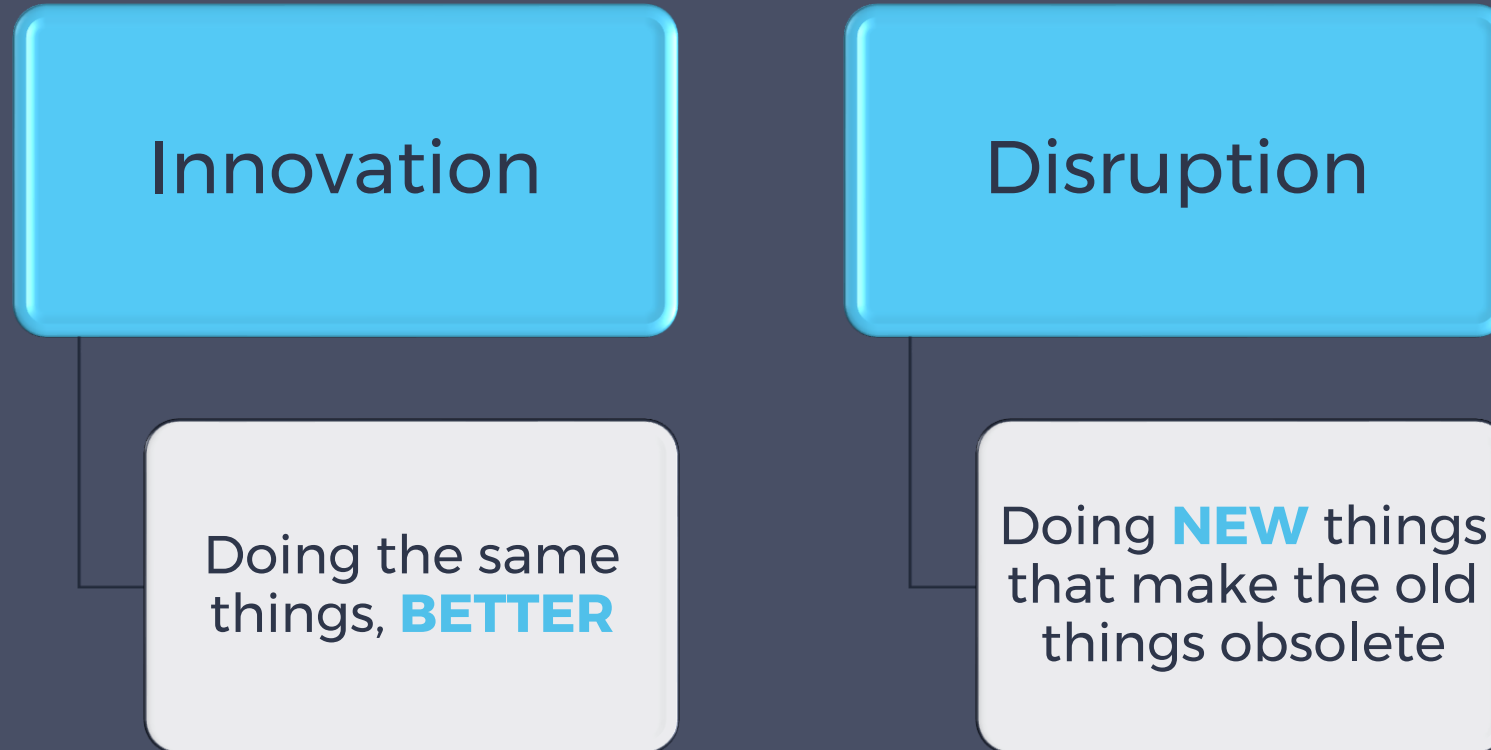
Current Landscape

9



Innovation vs. Disruption

Organizations must harness the chaos of continuous change



Risk Considerations

Digital Transformation Risk

- More organizations are embracing modern technology than ever before
- Each year more goes from physical to digital

Digital Transformation - the integration of digital technology into all areas of an organization changing how you operate and deliver value.

1. Third Parties
2. Operational Resilience
3. Internet of Things





Cybersecurity and Preventing Fraud

- As IT evolves, so do the schemes used by hackers
- Prevent unauthorized access to your network
- Monitoring and evaluation
- Protect sensitive data (PII, financial, IP, etc.)
- Consequences of a breach can be catastrophic (loss of money, loss of data, reputational damage, etc.)





vmware®
Carbon Black



SOPHOS



Next-Gen Anti-Virus



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



Recent Events



Increase in Cyber Events

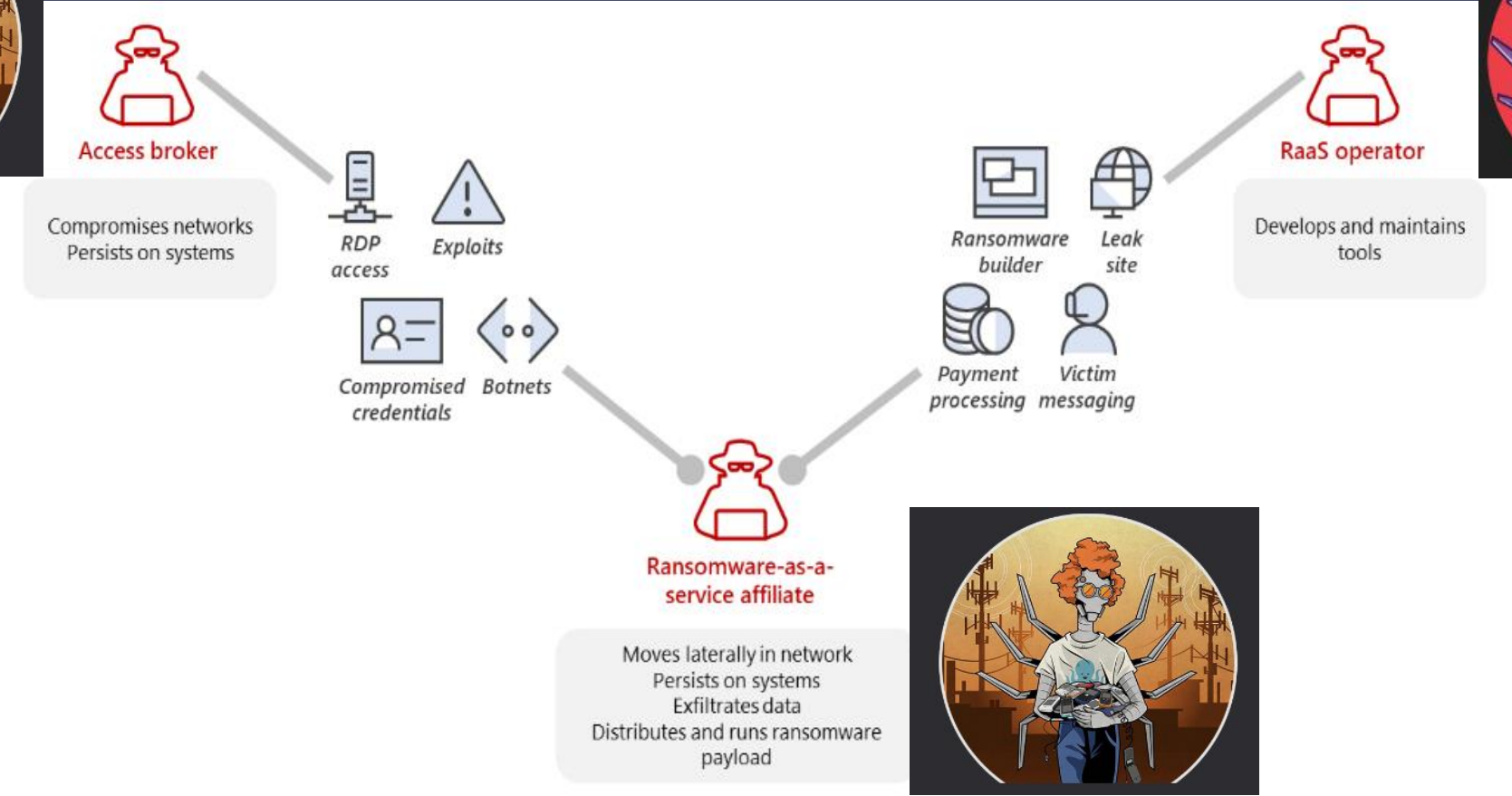


Scattered Spider



ALPHV or Alpha Spider

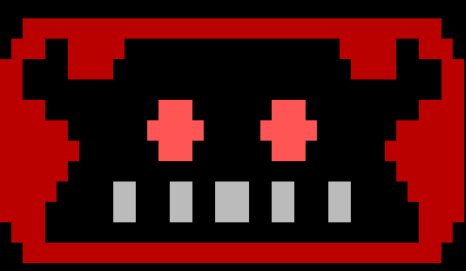
Ransomware-as-a-Service (RaaS)



Source: Microsoft & CrowdStrike



Scattered Spider



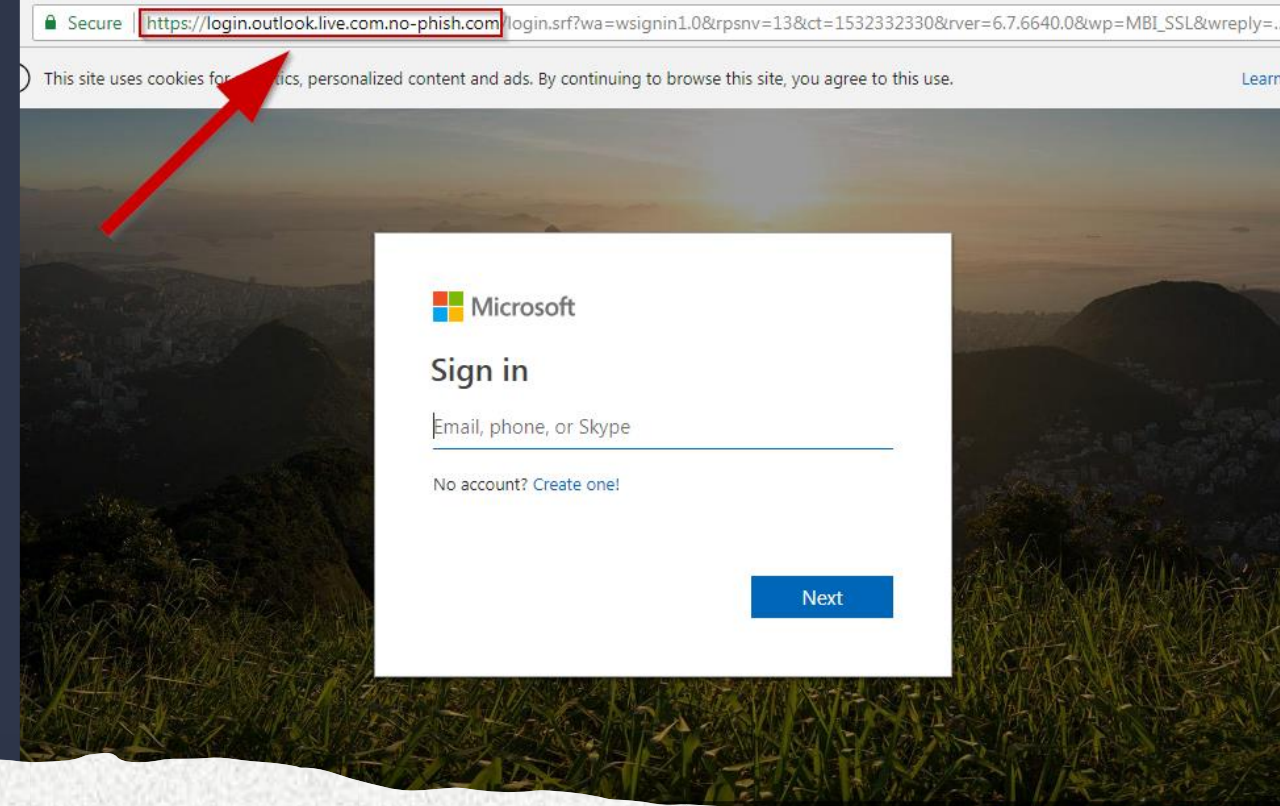
Evilginx

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	@jamescillum	disabled	available	
protonmail	@jamescillum	disabled	available	
protonmail mobile	@white_fi	disabled	available	



Example of Social Engineering



What can happen

```
[09:28:46] [imp] [0] [redacted] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36 (redacted)
[09:28:46] [inf] [0] [redacted] landing URL: https://accounts.docs.redacted.com/signin/v2/identifier?hd=dUp4&ol=aHR0cHM6Ly93d3cuZHJvcC5jb20=
[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	[redacted]	[redacted]	[redacted]	captured	[redacted]	2018-07-16 09:29

: sessions 1086

```
id : 1086
phishlet : [redacted]
username : [redacted]
password : [redacted]
tokens : captured
landing url : https://accounts.docs.redacted.com/signin/v2/identifier
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.redacted.com","expirationDate":1563269413,"value":"1:SeA2lf_9K9cYes1sK-Zxf4IJYbFuExL7kzR7NhRKJymxHJibcsGMQxlTNJ-EhkDGZ00kluJYWfu3leP-pKgmI5z0_g:ZYrZlHOEDfcAX0TT","name":"GAPS"}, {"path":"/","domain":"accounts.redacted.com","expirationDate":1563269413,"value":"PwaNHSJvu9q3BIuKdp-VGNWP6pa78vOk1AAkiC41dU8QVT27WFnHFUAdxeqkwqTJQzdcw","name":"LSID"}, {"path":"/","domain":"redacted.com","expirationDate":1563269413,"value":"7aV8JVGvGF1dty0x/AmWcSzaItWrT1JhsD","name":"APISID"}, {"path":"/","domain":"redacted.com","expirationDate":1563269413,"value":"","name":"sessionid"}]
```



Understanding

AI

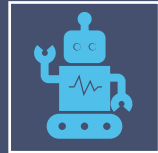
19



Definition of AI



A machine-based system that can for a given set of human-defined objectives, make predictions,



recommendations or decisions influencing real or virtual environments. Artificial intelligence systems



use machine and human-based inputs to:



a. Perceive real and virtual environments.



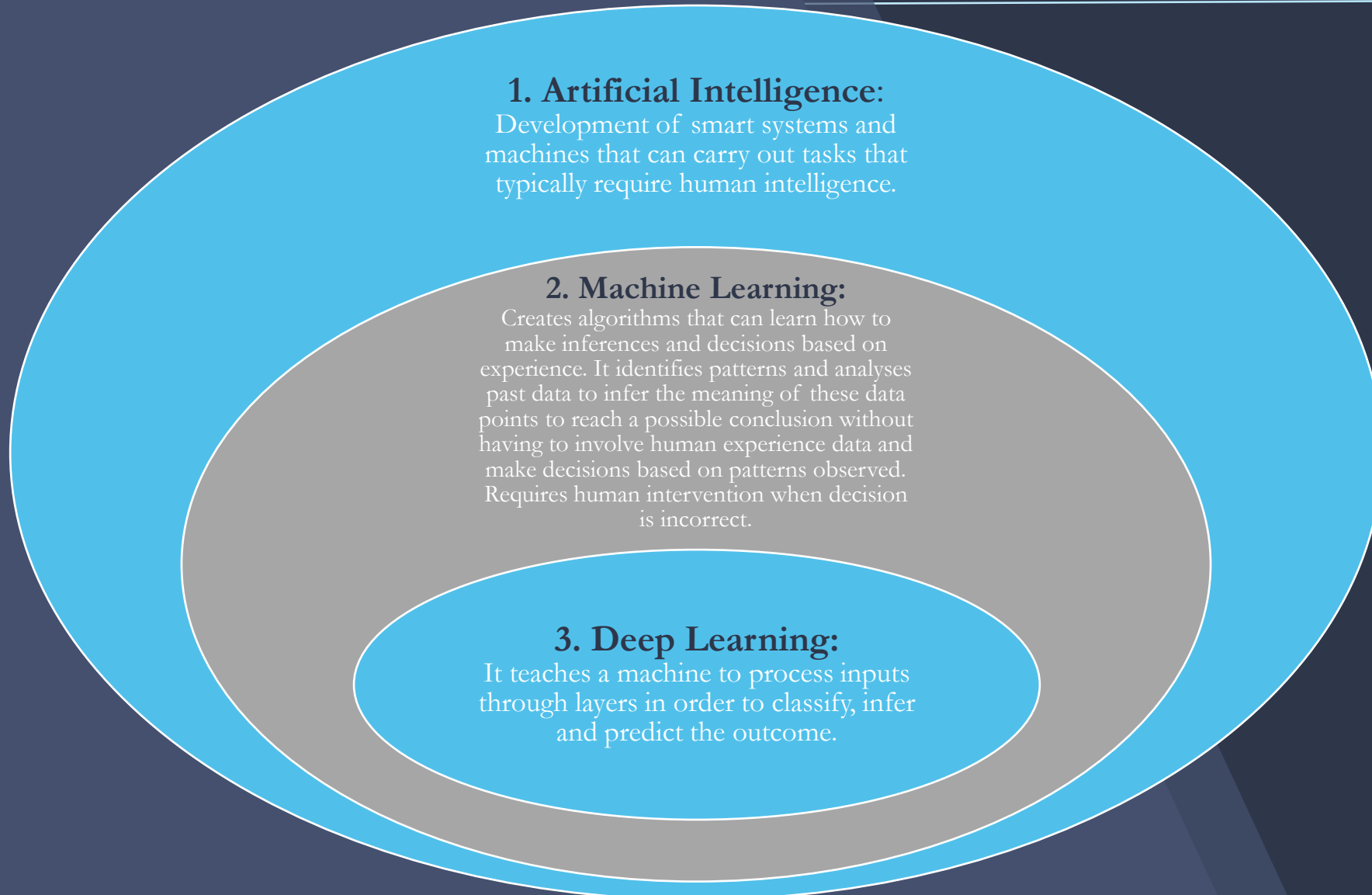
b. Abstract such perceptions into models through analysis in an automated manner.



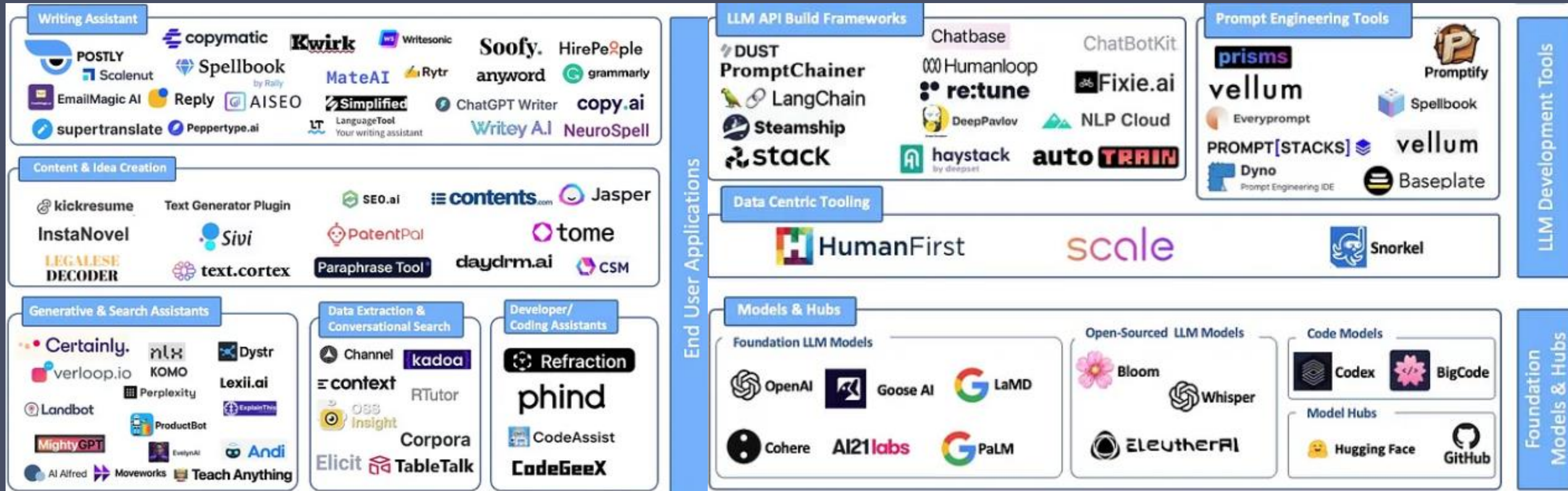
c. Use model inference to formulate options for information or action.



Current Landscape – AI vs ML



Foundation Large Language Model Stack



How AI and other tech can help in the Cybersecurity Pathway

23



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?



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>



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



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



Email / Username	Leaked Info	Password Type	Severity
rob.hand@kaseya.com	****	PLAIN	Critical CWSS: 8
rob.hand@kaseya.com	1e****	HASH	Critical CWSS: 8


Credential Management

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



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
```



Polling Question #2

Does your organization follow an IT security framework?

- A. *ISO*
- B. *NIST Cybersecurity Framework (CSF)*
- C. *NIST CMMC (Government Contractor)*
- D. *PCI-DSS*
- E. *Multiple Frameworks*
- F. *None*
- G. *Unsure*



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





AI Gone Rogue

AI should be the
start not the
end result



ChatGPT



AI assisted Report Writing

Add Recommendations ⓘ

Allow Automated Recommendation ⓘ

Audience ▼

- Cybersecurity Professional
- Technical
- General Business
- Common Language

Implement

Add F

Level of Detail ▼

- Brief
- Adequate
- Expansive

A Cybersecurity Professional = Uses language specific to solutions and terms commonly used in the cybersecurity industry that may be difficult to understand by users outside of cybersecurity.

A Technical Expert = Intended to help users with a technical background (such as solution engineers, development resources, and product owners) implement solutions related to a specific subcontrol.


A General Business User = Uses language understandable by a user with working business knowledge inside of the organization the assessment is being performed for.

In Common Language = Intended to be understood by anyone with or without prior knowledge on the compliance framework associated with the assessment.



AI assisted Report Writing cont...

Do you ensure third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities?

Subcontrol: Third Party Stakeholders (PR.AT-3) 

- Yes
- No
- Partially
- Not Applicable
- I don't know

Enter notes

To ensure third-party stakeholders understand their roles and responsibilities, it is crucial to establish clear communication channels and documentation. First, develop a comprehensive onboarding process that includes a thorough explanation of their specific roles and responsibilities related to cybersecurity. Provide them with relevant policies, guidelines, and training materials tailored to their needs. Regularly conduct review sessions and assessments to ensure their understanding and address any gaps or concerns. Additionally, establish continuous communication channels to keep them informed about any changes or updates in cybersecurity practices and encourage collaboration for improved security posture.



AI assisted Report Writing cont...

Do you ensure third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities?

Subcontrol: Third Party Stakeholders (PR.AT-3) ⓘ

- Yes
- No
- Partially
- Not Applicable
- I don't know

Enter notes

To ensure that third-party stakeholders comprehend their roles and responsibilities, it is advisable to establish clear and concise communication channels and provide comprehensive documentation that outlines their specific tasks and obligations. Regular meetings and training sessions can also be organized to address any concerns, fostering a strong understanding and collaboration between all parties involved.



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



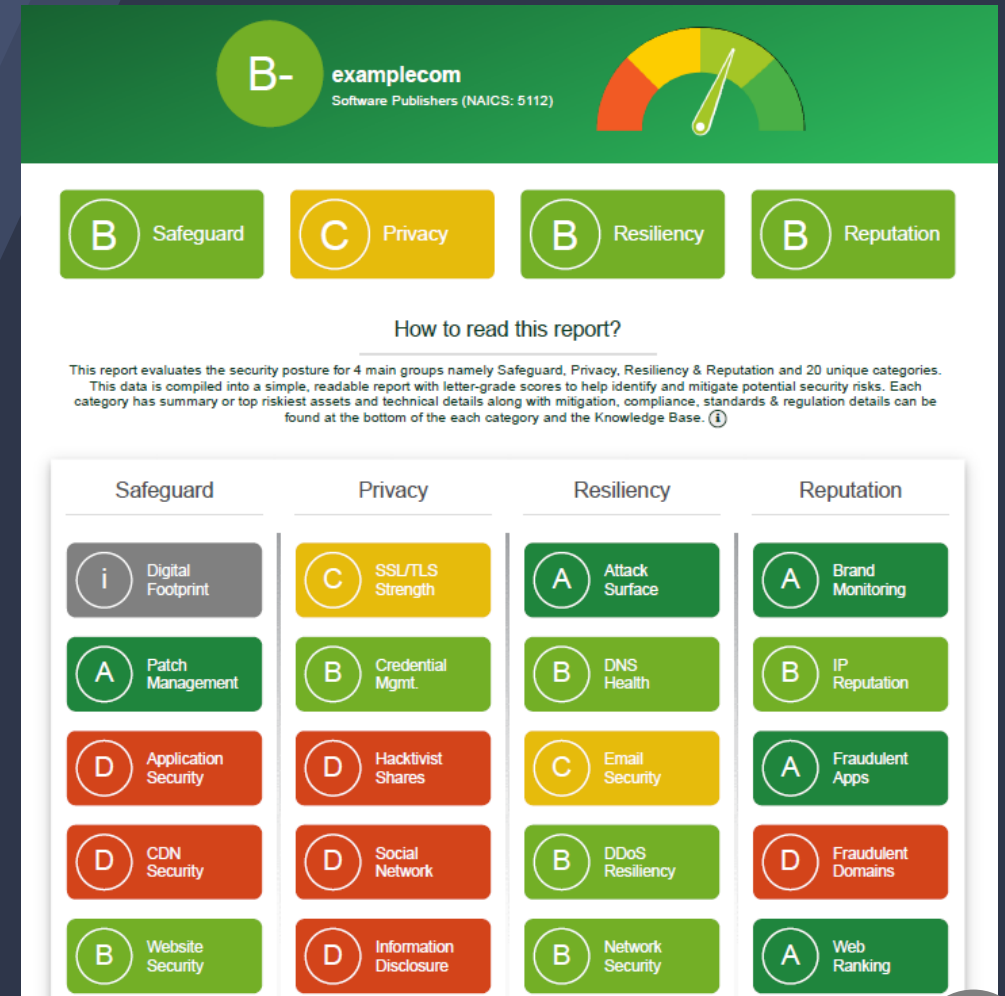
Embracing Technology

Data Breach Index (DBI): **0.877** ⓘ



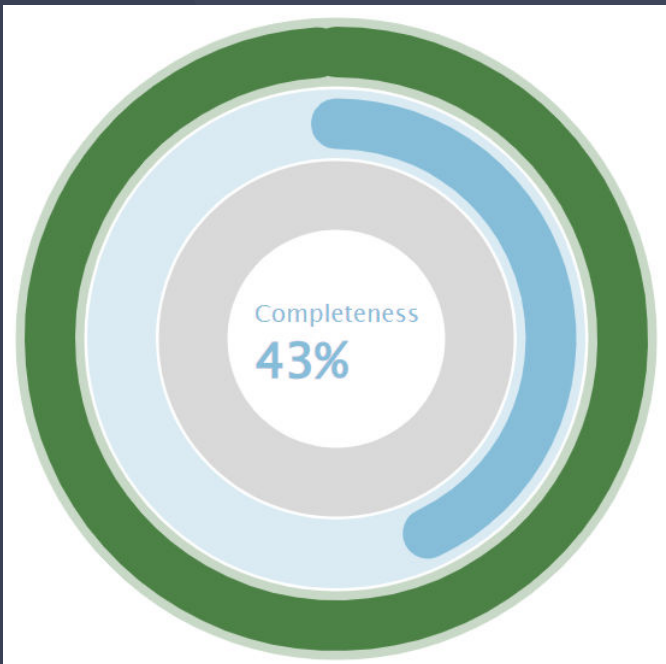
Ransomware Susceptibility Index (RSI): **0.238** ⓘ ?

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



AI with third party risk management

📊 Estimated **NIST Cybersecurity Framework (CSF)** Level: **99%**



Area	Result	Completeness
DE.AE Anomalies and Events	100%	20%
DE.CM Security Continuous Monitoring	99%	75%
DE.DP Detection Processes	100%	20%
ID.AM Asset Management	93%	33%
ID.BE Business Environment	100%	20%
ID.GV Governance	100%	75%
ID.RA Risk Assessment	98%	50%
ID.RM Risk Management Strategy	N/A	0%



AI with 3rd Party Risk Management

 Estimated NIST Cybersecurity Framework (CSF) Level: **99%**

Compliance Mapping of CSF>PR.DS-1

Description:

Data-at-rest is protected



Item CIS v8>3.4

Compliance Output 5/5

Confidence 73%

Description Enforce Data Retention Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.

Relation Similar content(s) found in privacypolicies/[redacted].com:

- We will retain your information for as long as your account is active, as needed to provide you the [redacted] Product, and/or as provided by law. After your account is closed, we may continue to communicate with you about [redacted] Products or give you important business updates that may affect you unless you have opted out of receiving such communications. If you wish to request that we no longer use your information to provide you [redacted] Products, contact us through the online portal. We will retain and use your information as necessary to comply with our legal obligations, for security and fraud prevention, to resolve disputes, and enforce our agreements. We set retention timeframes based on the type of data.



YOU ARE HERE 0.47

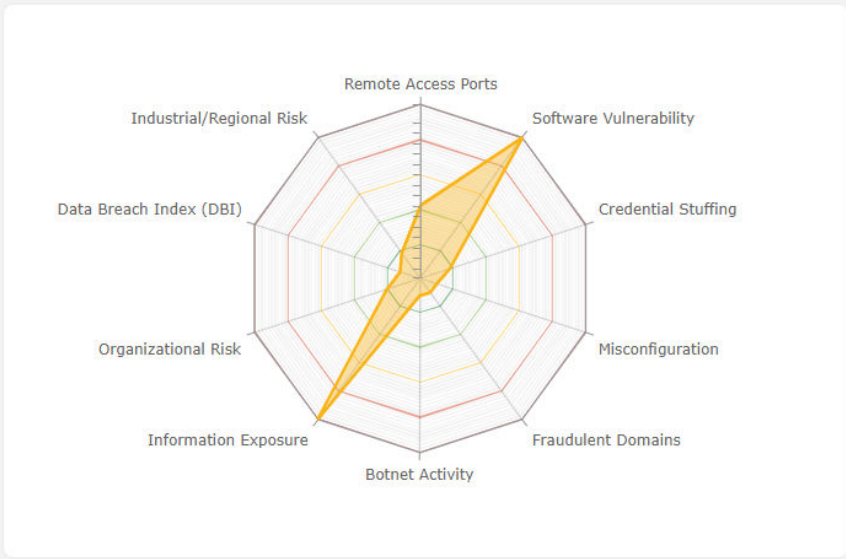


INDUSTRY AVERAGE

Ransomware Indicators

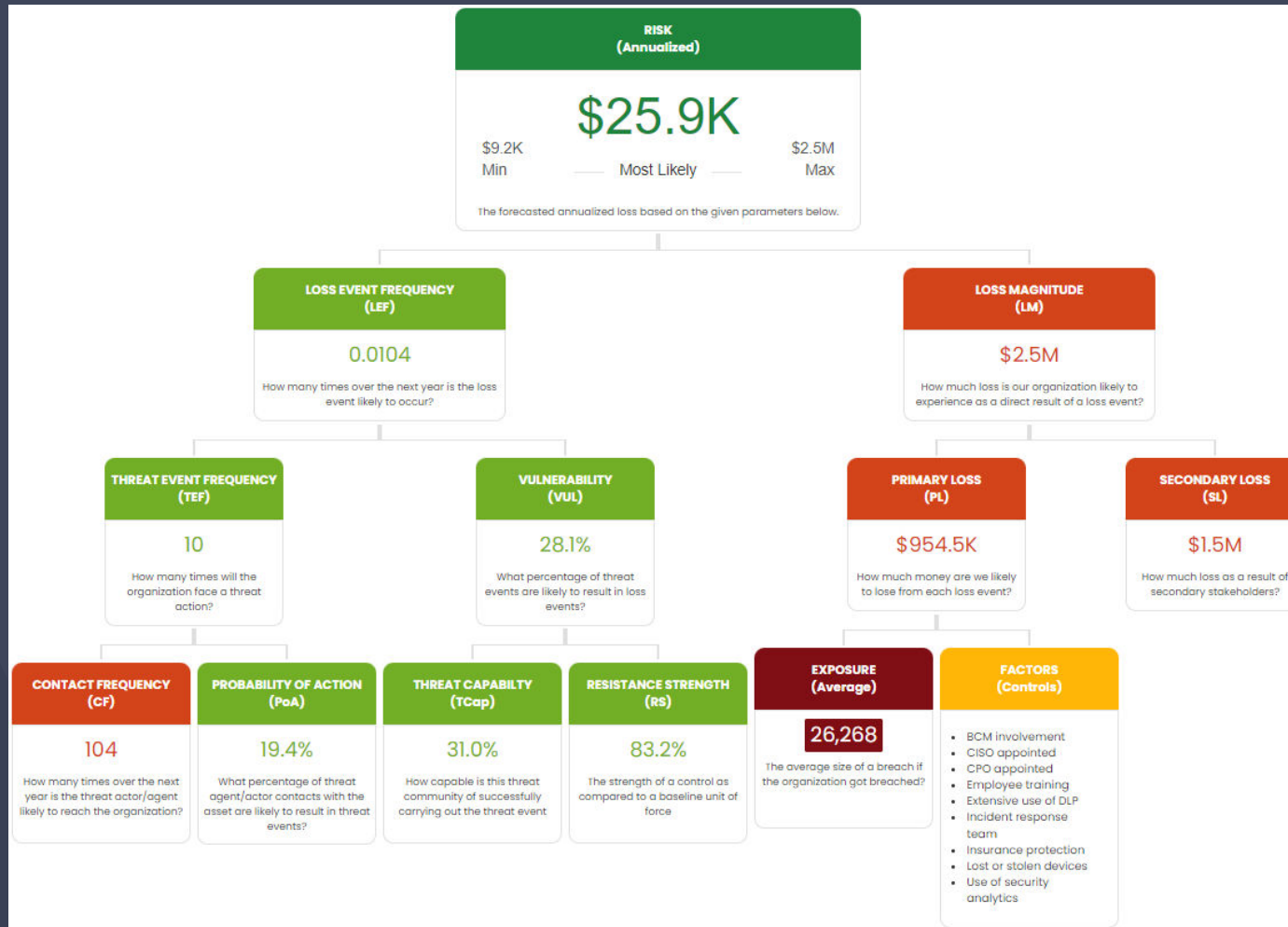
Remote Access Ports:	1 finding
Software Vulnerability:	25 findings
Credential Stuffing:	233 findings
Misconfiguration:	Minimal
Fraudulent Domains:	30 findings
Botnet Activity:	Minimal
Information Exposure:	2 findings
Organizational Risk:	0.2
Data Breach Index (DBI):	0.12

Ransomware Radar



Ransomware Index & TPRM

FAIR Analysis



Culture

45



The Culture of Innovation

Innovation

- The process of introducing new ideas, devices or methods to solve problems

Culture

- The way of thinking, behaving and working that exist in an organization

Culture of Innovation

- Nurturing an environment that continually induces new ideas or ways of thinking then translates them into action to solve problems or seize opportunities



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/>

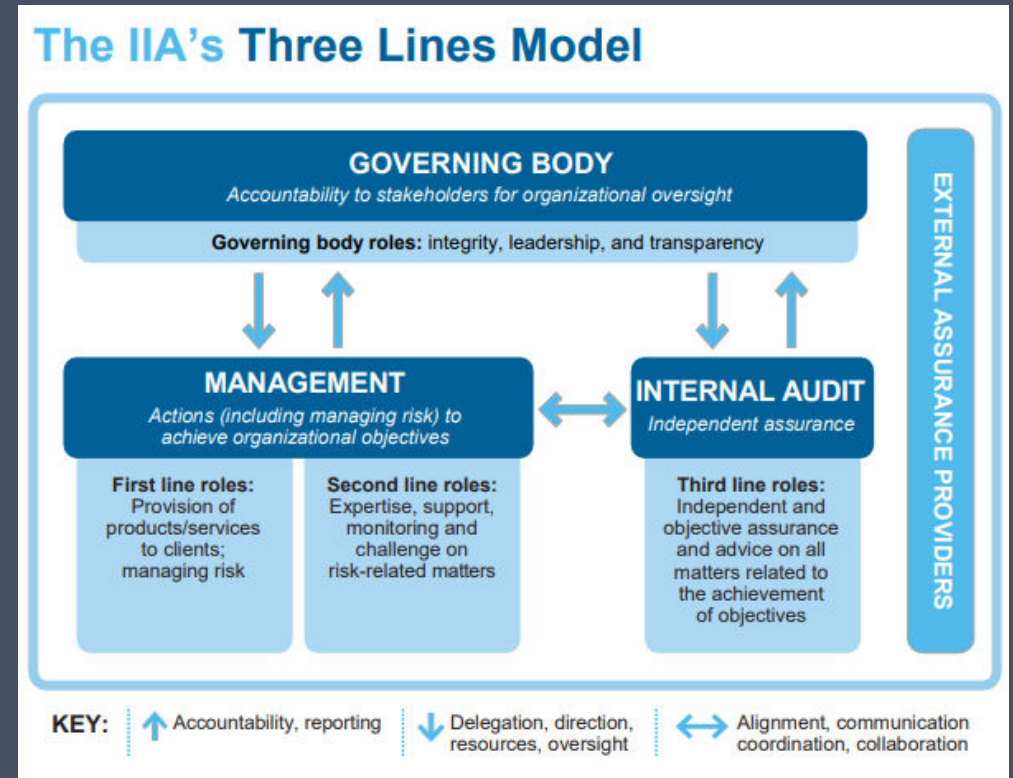
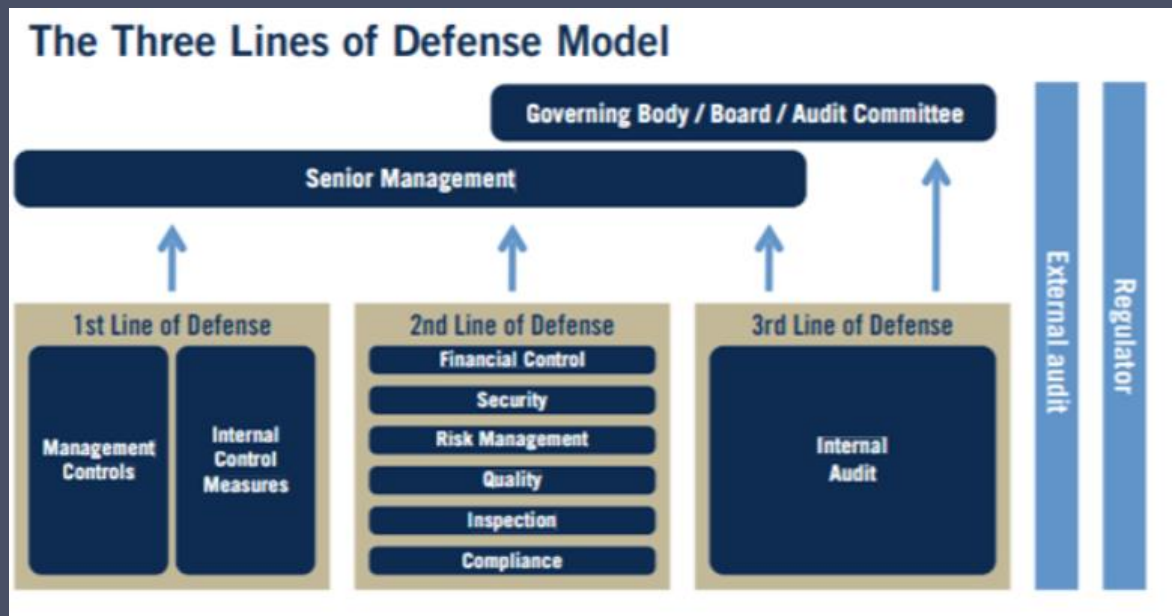


IIA's new "Three Lines Model" stresses collaboration

Previous Model



Updated Model



The new "Three Lines Model," as it is now referred to by the IIA, "acknowledge[es] that risk-based decision-making is as much about seizing opportunities as it is about defensive moves," [the organization stated in a press release](#). "The new Three Lines Model helps organizations better identify and structure interactions and responsibilities of key players toward achieving more effective alignment, collaboration, accountability and, ultimately, objectives." – [July 20, 2020](#)



Polling Question #3

Is your board actively engaged in your organization's top risks?

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



CCPA Drafted Regulations

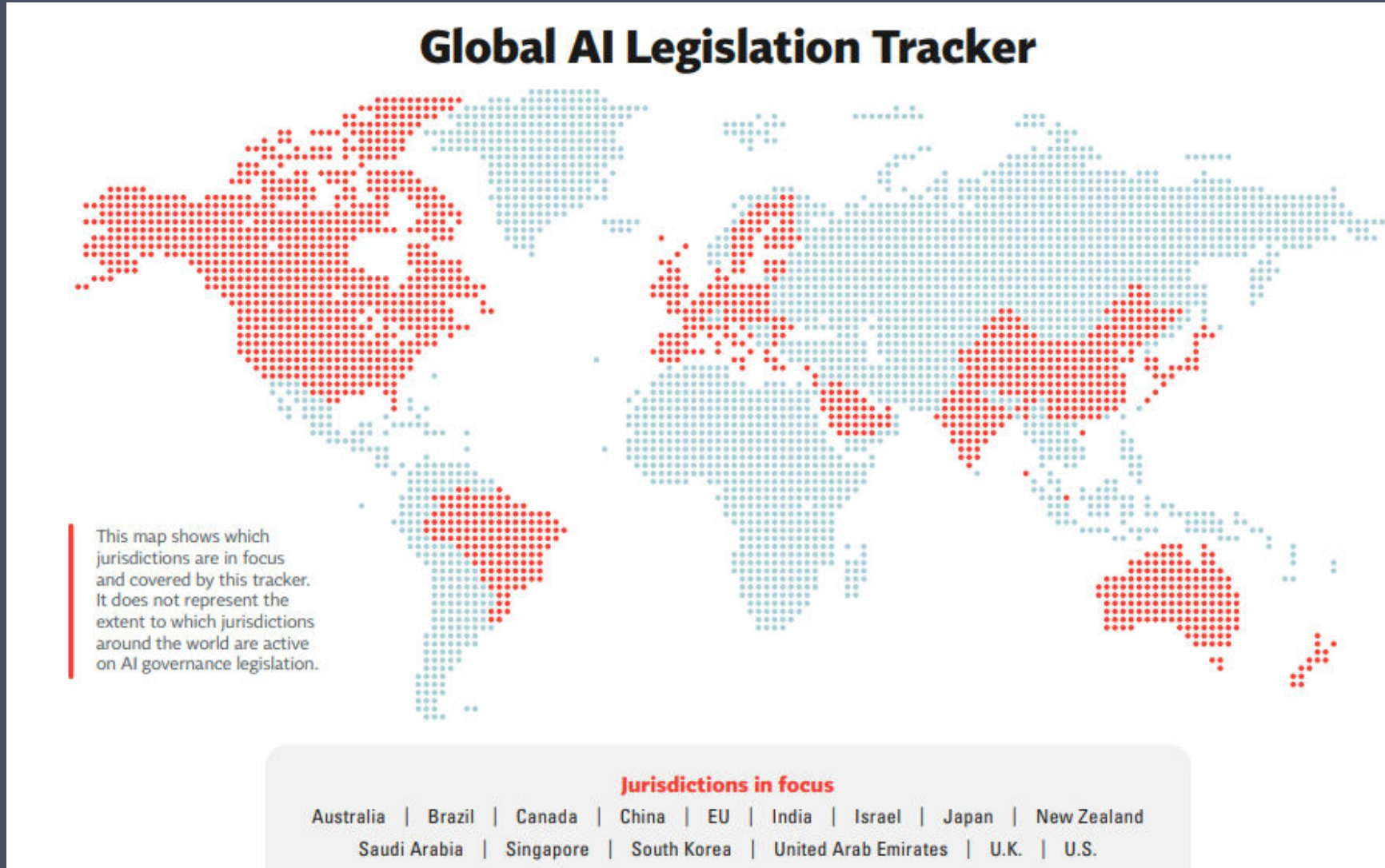
50

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



Global AI Legislation Tracker





**Want more?
Check out
our podcast!**



Presenters

Meet the Instructors



Melissa Musser,
CPA, CITP, CISA, CIA

mmusser@grfcpa.com
301-951-9090



Ricardo Trujillo
CPA, CITP, CISA

rtrujillo@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.