When Social Media Platforms & Social Engineering Crimes Collide

Thursday, September 10 @ 11 AM Eastern

Gallagher

Advisen
Transforming • Insurance℠

Today's webinar is sponsored by:

Gallagher

Advisen
Transforming • Insurance℠

When Social Media Platforms & Social Engineering Crimes Collide:
Securing your business and your personal privacy

Visit **www.advisenltd.com** at the end of this webinar to download:

- Copy of these slides
- Recording of today's webinar

Mark your Calendars!

Register for all upcoming webinars at
www.advisenltd.com/media/webinars

Advisen
Transforming • Insurance℠

ARE YOU A RISK MANAGER?

We have something just for you

Advisen
Transforming • Insurance℠

Today's Panelists

John Farley, CIPP/US

Managing Director, Cyber Practice

Gallagher

Dr. Chris Pierson
Founder & CEO

BLACKCLOAK

Adv!sen
Transforming • Insurance℠

When Social media Platforms and Social Engineering Crimes Collide

Cyber Risk Insight Webinar Series | September 10, 2020

Presenting with

BLACKCLOAK

Gallagher

Insurance | Risk Management | Consulting

John Farley, CIPP/US

Gallagher
Managing Director, Cyber Practice
(212) 763-3424
John_Farley@ajg.com

Dr. Chris Pierson

BLACKCLOAK
Founder & CEO
info@blackcloak.io

Presenting with

BLACKCLOAK

Agenda

I. Recent Social Media Platform Hacks & Wrongful Data Collection

II. Lessons Learned & Best Practices

III. The Government's Role

IV. Transferring the Risk – Cyber Insurance

V. Questions

Presenting with

BLACKCLOAK

Recent Social Media Platform Hacks &

Wrongful Data Collection

Part I.

Presenting with

BLACKCLOAK

Overall Threats & Risks

- Overcollection

- Appropriate Use

- Internal Access

- Security of the Data

- Onward Use (3rd Parties)

Presenting with

BLACKCLOAK

Twitter

- What Happened?

- Internal Administration

- 2 Issues:
  - External (Reputational)
  - Internal (Security/Rep.)

- Social Engineering Risks

- Heightened post-Covid Risk
  - Remote workforce
  - Training & Education

Gallagher
Insurance | Risk Management | Consulting

Presenting with

BLACKCLOAK

Zoom

- What happened?
  - Extended Use
  - No training, controls hard, different end-user
- Audience matters
- Lack of Business Continuity Planning/Disaster Recover
- Culture of No
- Settings, Settings, Settings

Presenting with

BLACKCLOAK

Facebook

- **What happened?**
  - Data Collection
  - Onward Use
  - Third-Party Assurance
- Acknowledging lack of attention & ownership of data/privacy policies
- Accountability to "Say what you do, do what you say."

Presenting with

BLACKCLOAK

Lessons Learned & Best Practices

Part II.

Presenting with

BLACKCLOAK

The User

- Settings Matter:
  - Privacy Settings
  - Security Settings
- Contracts:
  - Review them or decide to own uses of your info

Presenting with

BLACKCLOAK

Specifics

- Privacy:

  - Use of info by the company

  - Use of info by Third-Parties

  - Settings for ads, sales, etc.

  - Your cookie/tracking settings

- Security:

  - Dual Factor Authentication

  - Strong Passwords

  - Encrypted Password Vaults

  - Reviews of Logins

Presenting with

BLACKCLOAK

Vendor Management

Create a vendor management program focusing on:
- ✓ Regulatory compliance
- ✓ Mitigation of legal / business / reputational risk

- Require periodic cyber risk assessments / vulnerability scans / penetration tests

- Require employee background checks & training.

- Address roles & responsibilities in breach response.

- Insurance and indemnification language.

- Have a contingency plan to use alternate vendors.

- Document gaps and rank your vendors from best to worst.

- Consider aggregation risk.

Presenting with

BLACKCLOAK

The Government's Role

Part III.

Presenting with

BLACKCLOAK

Guide or Owner

- Two Audiences:
    - For Government
    - For The People
- Guide & Warnings
- Outright Embargos
- Global Commerce
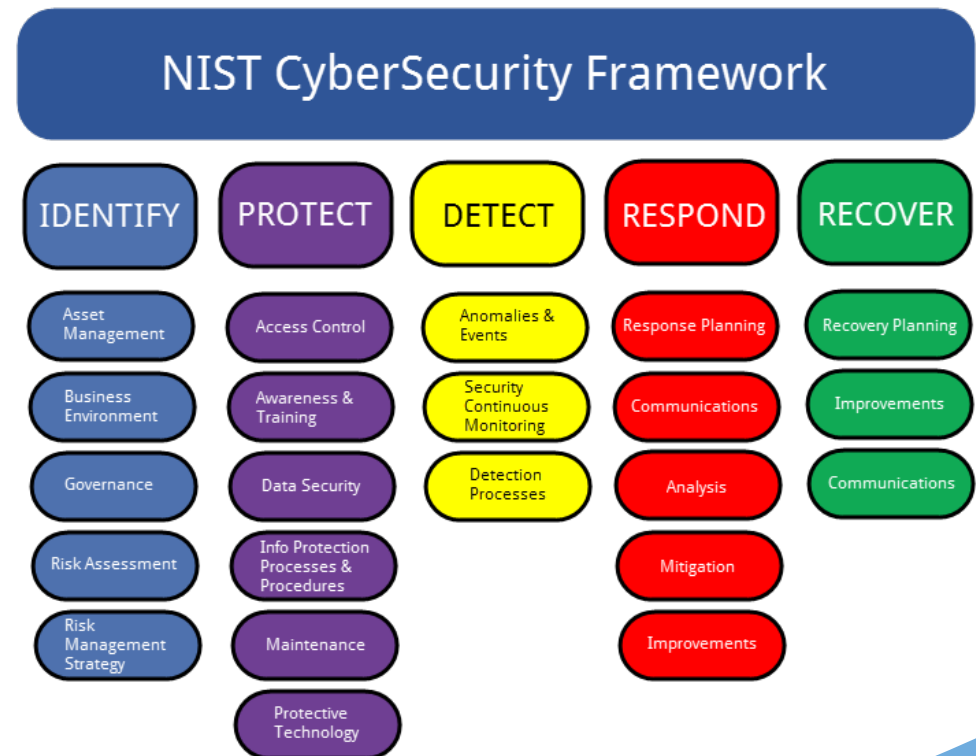- Whack-a-Mole
    - How does this scale?

Presenting with

BLACKCLOAK

Guidance Roles

- NIST Guidance
- Use by the Private Sector
- Creating your own risk framework
- Can apply to any business, sector, and even individuals

NIST CyberSecurity Framework

IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Access Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes & Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Presenting with

BLACKCLOAK

Transferring the Risk – Cyber Insurance

Part IV.

Presenting with

BLACKCLOAK

Business Interruption Claims

- Waiting Periods – approximate range: 8 to 12 hours
- Period of Restoration – approximate range: 90 to 120 days

Security failure - unauthorized access or use of computer systems & infection by malicious code.

System failure – unplanned & unintentional interruption of computer systems.

Presenting with

BLACKCLOAK

Contingent Business Interruption Claims

Security failure: "Dependent" security failure – usually full limit

System failure:
How is "computer system" defined?

Is voluntary shutdown covered?

Limited to certain types of providers?

✓ Non-IT vendors might be sub-limited, some provide full limit (must be scheduled). "Dependent" system failure is usually sub-limited.

✓ Broad infrastructure exclusions: ISP , utilities, securities exchanges. Social media platforms?

Wrongful Data Collection & Regulatory Risk

- Regulatory endorsements added / broad policy language

- Regulatory investigations, lawsuits and fines *in the absence of a data breach* may not be covered.

- Some policies are covering "system improvements": usually require a data breach; may mitigate regulatory claims.

- Many jurisdictions *will not allow* coverage for punitive damages.

Presenting with

BLACKCLOAK

What Questions Do You Have?

Presenting with

BLACKCLOAK

Thank you!

John Farley

(212) 763-3424
John_Farley@ajg.com

Dr. Chris Pierson

info@blackcloak.io

Presenting with

BLACKCLOAK

Gallagher

Insurance | Risk Management | Consulting

When Social Media Platforms & Social Engineering Crimes Collide:
Securing your business and your personal privacy

Visit **www.advisenltd.com** at the end of this webinar to download:

- Copy of these slides
- Recording of today's webinar

For more on Advisen, visit at
www.advisenltd.com or email us
at **webinars@advisen.com**

Leading the way to **smarter**
and more **efficient**
risk and insurance **communities**.

Advisen delivers:
the ***right information*** into
the ***right hands*** at
the ***right time***
to **power performance**.