



Playing Chess Against Nation-State and Ransomware Threat Actors

Tuesday, June 30th at 10 AM Eastern



CROWDSTRIKE



Today's webinar is sponsored by:



CROWDSTRIKE





Playing Chess Against Nation-State and Ransomware Threat Actors

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

- Recording of today's webinar
- Copy of Slides

Mark your Calendars!



 **LIVE WEBINAR**

Property: A Moving Target

Tuesday, July 7 @ 11 AM ET

 **Advisen**
Transforming • Insurance™

REGISTER NOW



 **LIVE WEBINAR**

Thursday, July 16 at 11am ET

Balancing Risk with Cyber Insurance:

Through the
eyes of the CIO

REGISTER NOW

SPEAR TIP
CYBER COUNTERINTELLIGENCE



 **Advisen**
Transforming • Insurance™

Q3 2020 CYBER RISK TRENDS

WED, NOV 04 @ 11AM ET

LEARN MORE

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

ARE YOU A RISK MANAGER?

We have something just for you



**Risk Managers and Insurance
Buyers now get FPN Pro FREE**

LEARN MORE

Today's Moderator



Chad Hemenway

Managing Editor

Advisen

Email at chemenway@advisen.com

Today's Panelists



Josh Burgess

Strategic Threat Advisor
CrowdStrike



Chris Cwalina

Global Co-Head of Data Protection
Privacy and Cybersecurity
**Norton Rose Privacy
/Security Counsel**



Scot Lippenholz

Director of Incident Response
CrowdStrike



CROWDSTRIKE

ADVISEN

PLAYING CHESS AGAINST NATION-STATE AND RANSOMWARE THREAT ACTORS

JUNE 30, 2020

CROWDSTRIKE SERVICES

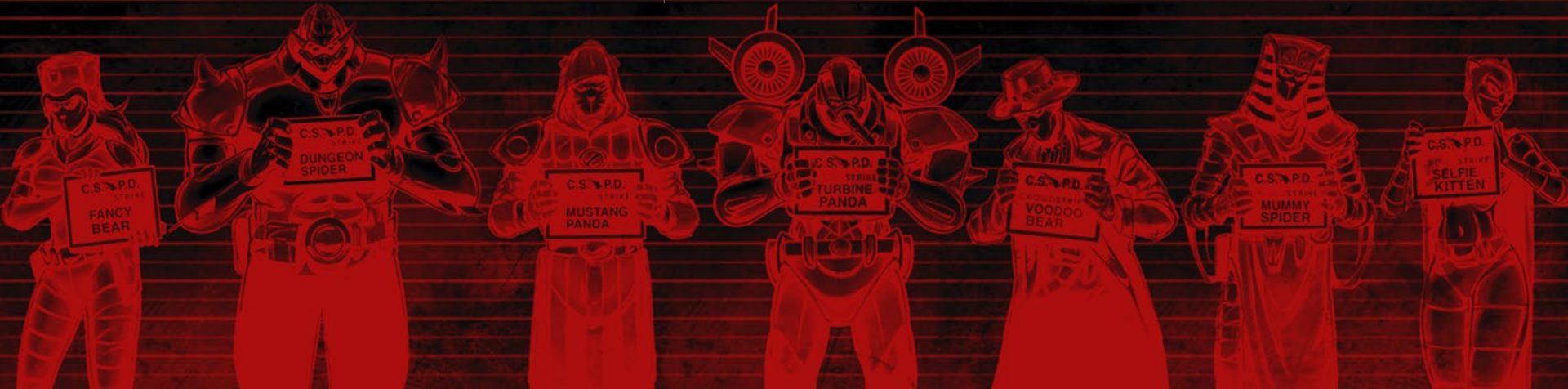
SCOT LIPPENHOLZ, JOSH BURGESS & ADAM COTTINI

NORTON ROSE FULBRIGHT US LLP

CHRIS CVALINA

AGENDA

- Threat Environment From the Front Lines
- Threat Actors
- Remote Incident Response
- Prevention and Recovery
- Legal Obligations and Key challenges
- Q&A





A LOOK AT THE THREAT ENVIRONMENT FROM THE FRONT LINES



DWELL TIME

2017	2018	2019
86 days	85 days	95 days

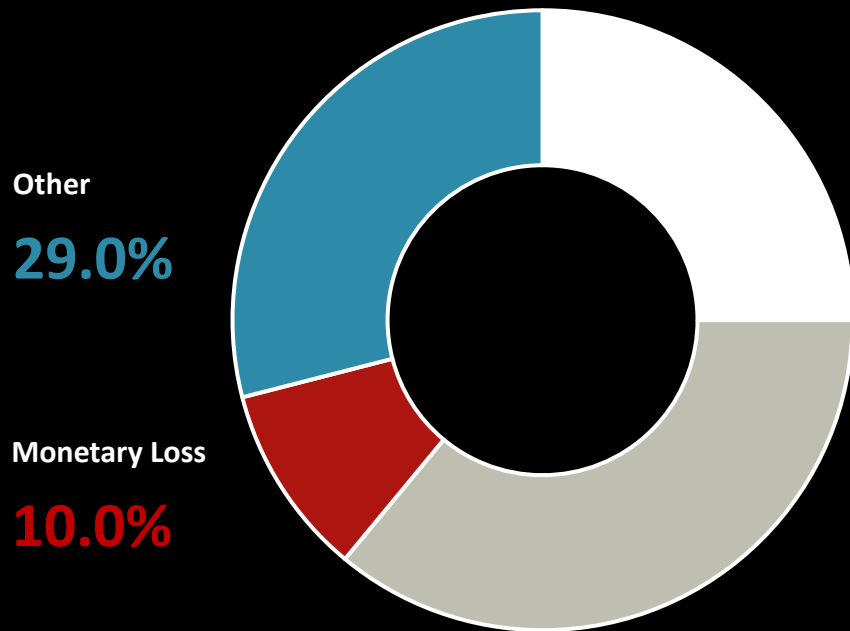
Dwell Time	% of Cases
< 1 day	16%
2 days to 1 week	13%
1 week to 1 month	23%
1 to 3 months	26%
3 to 6 months	13%
6 months to 1 year	3%
> 1 year	6%

“2019 data showed an increase to an average of 95 days that adversaries were able to hide their activities from defenders”



ATTACK IMPACTS

ATTACK IMPACT PER TYPE OF DAMAGE INCURRED



Data Theft
25.0%

BUSINESS DISRUPTION

- Ransomware
- Destructive Malware
- Denial of Service

DATA THEFT

- Intellectual Property (IP)
- Personally Identifiable Information (PII)
- Personal Health Information (PHI)

MONETARY LOSS

- Crimeware
- Formjacking
- Cryptojacking
- more

Business Disruption
36.0%



INITIAL ATTACK VECTORS

ATTACK VECTORS

- Spear-phishing
- Web Server Attack
- Compromised Credentials
- Supply Chain
- Other
- Unknown

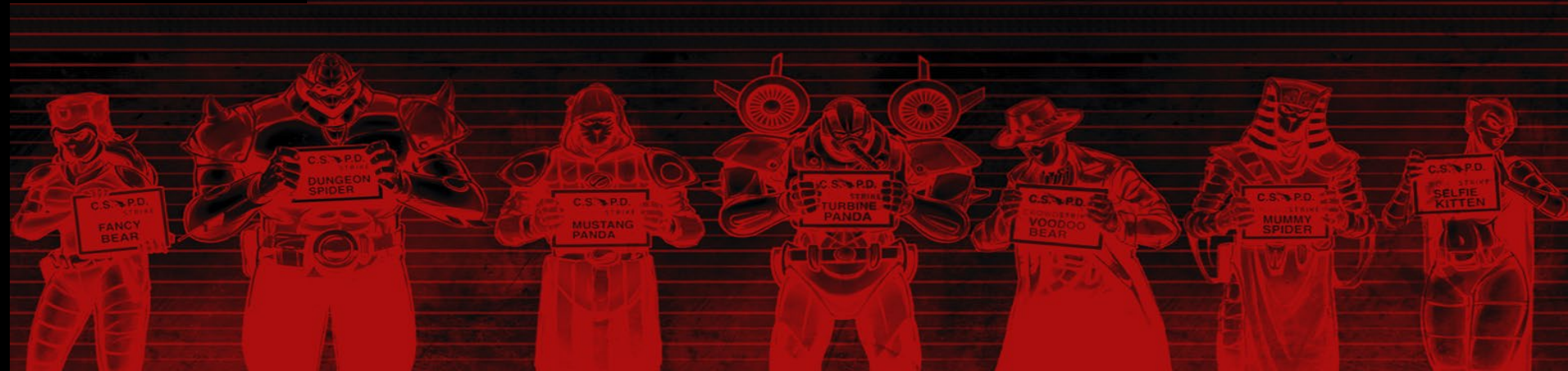
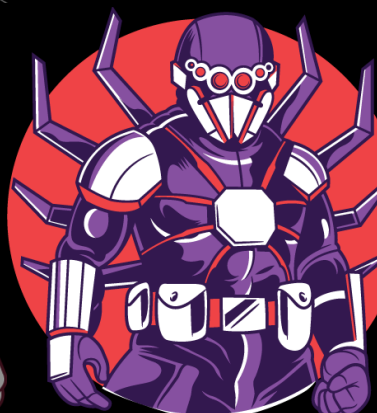
Category	2018	2019	MITRE ATT&CK Technique
Spear-phishing	33%	35%	<ul style="list-style-type: none">■ Attachment: 19%■ Link: 15%■ Service: 1%
Web Server Attack	20%	16%	<ul style="list-style-type: none">■ Exploit public facing application: 12%■ Drive by compromise: 4%
Compromised Credentials	20%	16%	RDP exposed, credential stuffing, publicly posted passwords
Supply Chain	Did not collect	6%	<ul style="list-style-type: none">■ Trusted relationships■ Supply chain: 1%
Other	12%	14%	Misconfiguration, commodity malware, false positive
Unknown	9%	14%	



Lions, and Tigers, and Bears oh my...



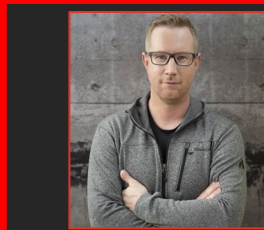
THREAT ACTOR LANDSCAPE



THE CYBER THREAT LANDSCAPE



HOW I BRIEF THREAT INTELLIGENCE



“What?”

*“Here is what I am
telling you”*

“So What?”

*“Here is why you
should care”*

“What Next?”

*“Here is what you
should consider doing about
it”*



STRATEGIC ASSESSMENTS



TURBINE PANDA IN ACTION



So What?

China is predicted to succeed the U.S. as the world's largest air travel market by 2022, two years ahead of schedule

Several Chinese initiatives and subsequent cyber capabilities focus on their long term strategic objectives including aerospace

What?

Chinese MSS targeted aerospace firms to siphon intellectual property related to the LEAP-X turbofan engines

A joint venture has been established by China and Russia to develop CR929 wide-body aircraft

What Next?

Do strategic goals from the 5 year plan, Belt and Road Initiative or Made in China 2025 plan align with your organization

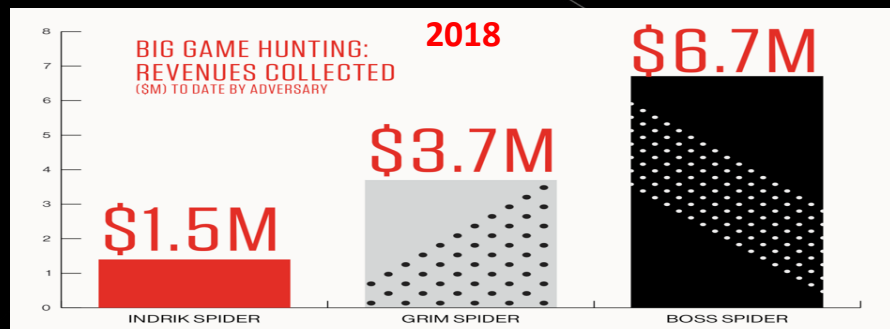
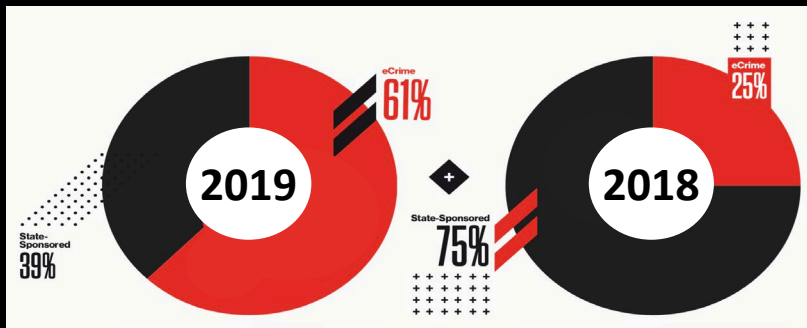
Understand your organizations footprint within and **assess the risks posed to your assets** that may be targeted by the mentioned nation-states



OPERATIONAL ASSESSMENTS



WHY IS RANSOMWARE AN ISSUE?

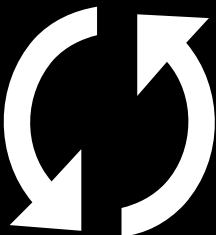


Why is this happening?

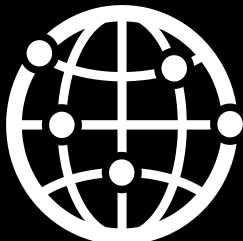
Strategy



Ecosystems



Attack Complexity



Between late 2018 and throughout 2019, Wizard Spider had collected a Grand Total of:



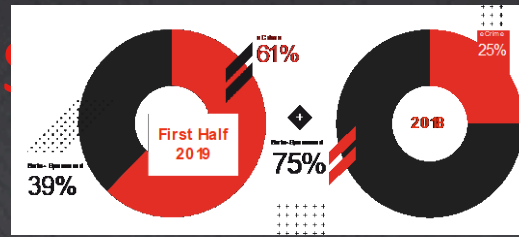
~\$100M USD
in Bitcoin



THREAT ACTORS



TYPES OF THREAT ACTORS



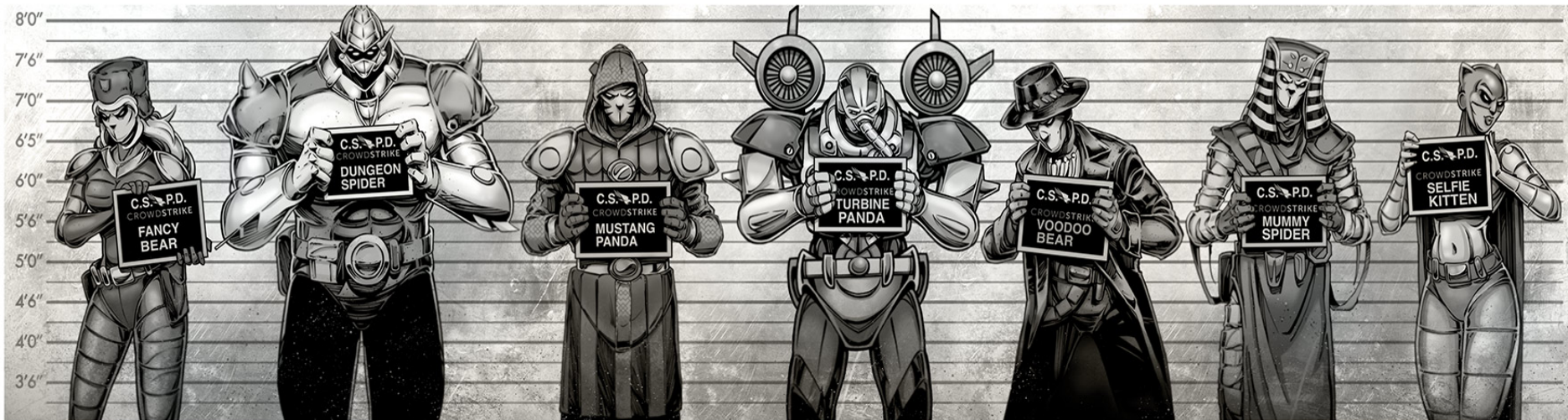
Capability For Damage



Threat Sophistication

ADVERSARIES ARE TAKING AIM AT YOUR BUSINESS

130+ active adversary groups tracked across the globe



500+ BILLION SECURITY EVENTS ANALYZED PER DAY 20+ MILLION INDICATORS ANALYZED PER DAY 35,000+ BREACHES STOPPED PER YEAR

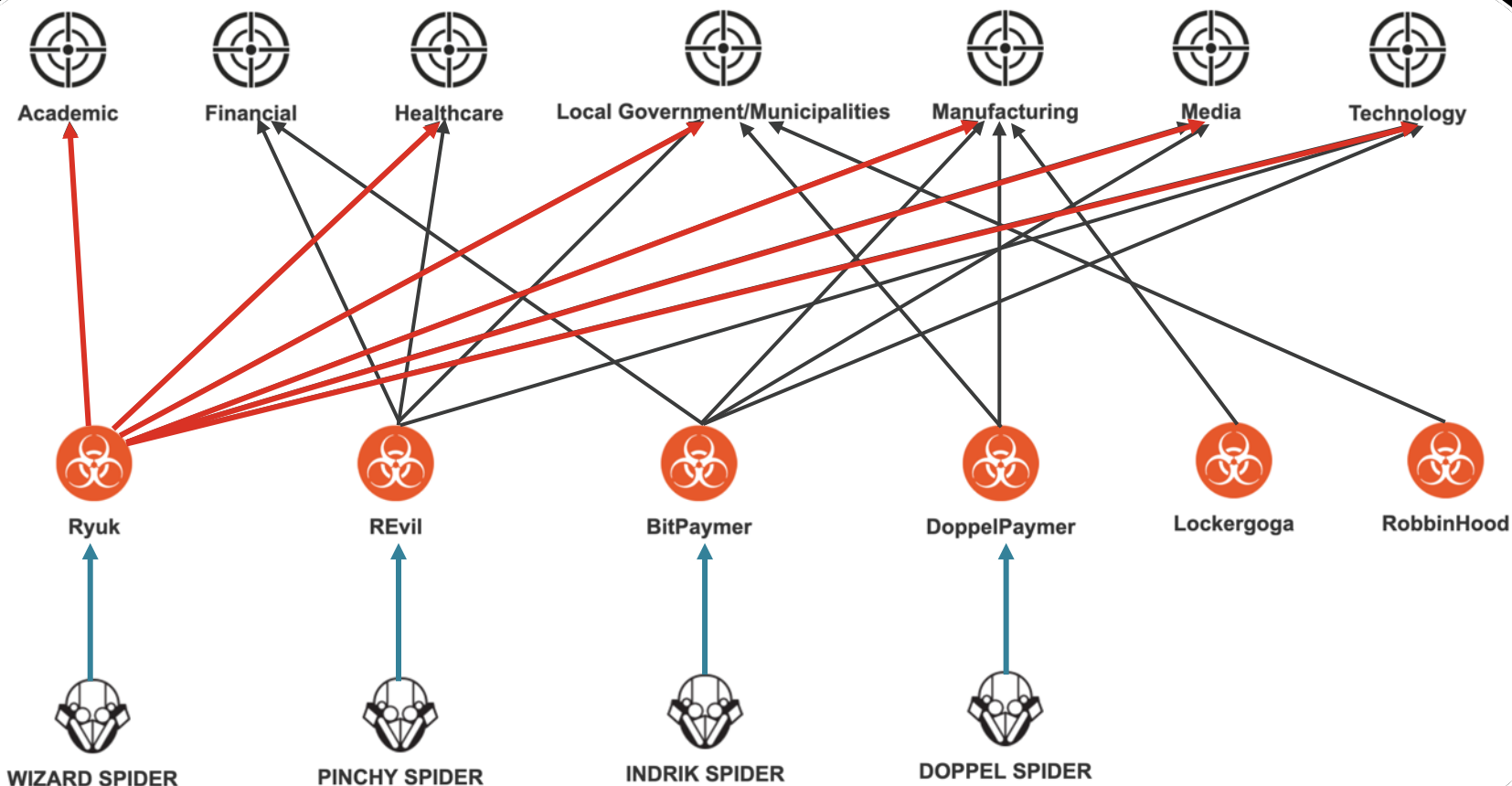


ECRIME TOP TREND: RICH GET RICHER

- Increase in the use of Malware-as-a-Service Operations
- eCrime actors are increasingly collaborating
- Ransomware continues to be threat of choice
- Hands-on activity increasingly observed



SECTOR TARGETING TRENDS





BGH FUTURE TRENDS

- New ransomware families (Cryakl / ProLock / NetWalker)
- Increase in incidents & number of sectors affected
- Improvements in cryptographic schemes (PWNDLocker weak crypto was replaced by ProLock)
- More criminal actors & improved operational security
- Maze Group started the trend of data theft & extortion or sale



LEGAL OBLIGATIONS AND KEY CHALLENGES



First significant GDPR fines and regulator focus

- Turnover-based fines under GDPR are now a reality
- Recently-announced fines are still TBC but are indicative of the DPAs' general approach
- These fines are being imposed primarily for what is deemed to be inappropriate / deficient security measures in place
- DPAs have particularly emphasised the need for:
 - Transparency - co-operation with the regulator is key
 - Appropriate technical and organisational measures to be in place
 - Analysis of supply chain risk
 - Cyber due diligence on acquisitions
- Regulators outside of EU/UK active
- US remains active but largely AG driven



KEY CHALLENGES IN GLOBAL INCIDENT RESPONSE

■ Issues

- Global strategy needs to be balanced with strict compliance objectives
- Securities Filings – requirements v. approach
- “Compliance” and “Obligations” mean different things in different regions / jurisdictions
- Approach different across the globe (US approach does not translate)
- Lack of vendors (call centre, mailing, credit monitoring)
- Notice content and Local language
- Formats for regulators vary significantly
- Questions vary
- Different timing requirements
- Cultural differences



KEY THEMES IN GLOBAL REGULATORY INVESTIGATIONS

- **Governance – cybersecurity program and privacy program***
- **Priority –** how to prove security/privacy a priority: budget and resources and preparation
- **Board of directors –** including decisions made and when informed
- **Risk Management function and decisions***
- Privilege assertions/challenges
- Supporting evidence
 - Controls
 - Policies, procedures, contracts
 - Prior knowledge: prior risk assessments; prior controls assessments, pen tests, audits, findings
 - Investigation materials: timelines; forensic reports, correspondence; minutes



CAPITAL ONE DECISION

- Issued May 26, 2020 by U.S. Magistrate Judge; request for reconsideration by Capital One denied by U.S. District Judge Anthony Trenga on June 25, 2020
- ACP/AWP at risk
- Consider:
 - Business as usual
 - Engagement terms and parties
 - MSSP use as IR firm
 - Report substance and delivery



Playing Chess Against Nation-State and Ransomware Threat Actors



Chad Hemenway
Advisen
[Moderator]



Josh Burgess
CrowdStrike



Chris Cwalina
Norton Rose Privacy
/Security Counsel



Scot Lippenholz
CrowdStrike

Thank You to our Panelists



Josh Burgess

Strategic Threat Advisor
CrowdStrike



Chris Cwalina

Global Co-Head of Data Protection
Privacy and Cybersecurity
**Norton Rose Privacy
/Security Counsel**



Scot Lippenholz

Director of Incident Response
CrowdStrike




Playing Chess Against Nation-State and Ransomware Threat Actors

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

- Recording of today's webinar
- Copy of Slides

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.**

About Advisen Ltd.

Advisen is the leading provider of data, media, and technology solutions for the commercial property and casualty insurance market. Advisen's proprietary data sets and applications focus on large, specialty risks. Through Web Connectivity Ltd., Advisen provides messaging services, business consulting, and technical solutions to streamline and automate insurance transactions. Advisen connects a community of more than 200,000 professionals through daily newsletters, conferences, and webinars. The company was founded in 2000 and is headquartered in New York City, with offices in the US and the UK.

+1 (212) 897-4800 | info@advisen.com | www.advisenltd.com