PROGRAM MATERIALS
Program #30289
December 14, 2020

Cybersecurity as Business Risk: Evaluating Cyber Risk in M&A

- Mark Sangster – Author of "No Safe Harbor" and eSentire VP Industry Security Strategies

Celesq® AttorneysEd Center
www.celesq.com

5255 North Federal Highway, Suite 310, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

Cybersecurity As Business Risk

Evaluating Cyber Risk in M&A

Celesq Attorneys Education Center| 14 DEC 2020

Mark Sangster

Principal Evangelist and VP industry Security Strategies

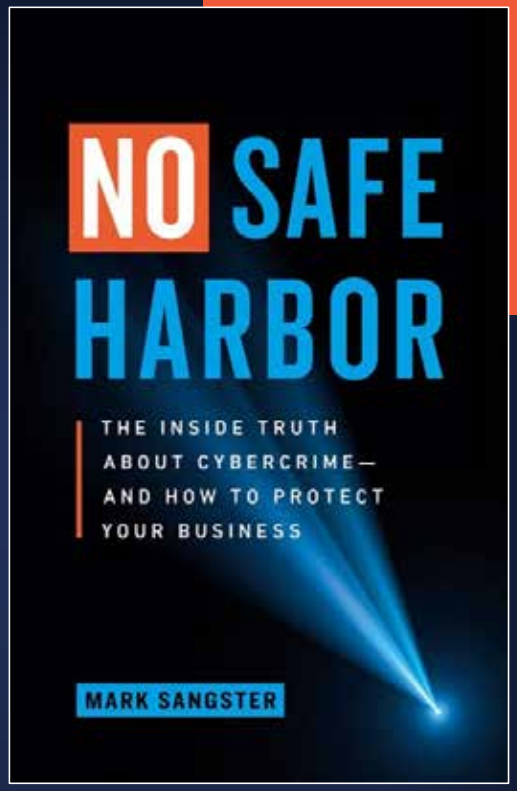
mark.sangster@esentire.com

@mbsangster

@cyber_mbsangster

Linkedin.com/in/mbsangster

mbsangster.com/book



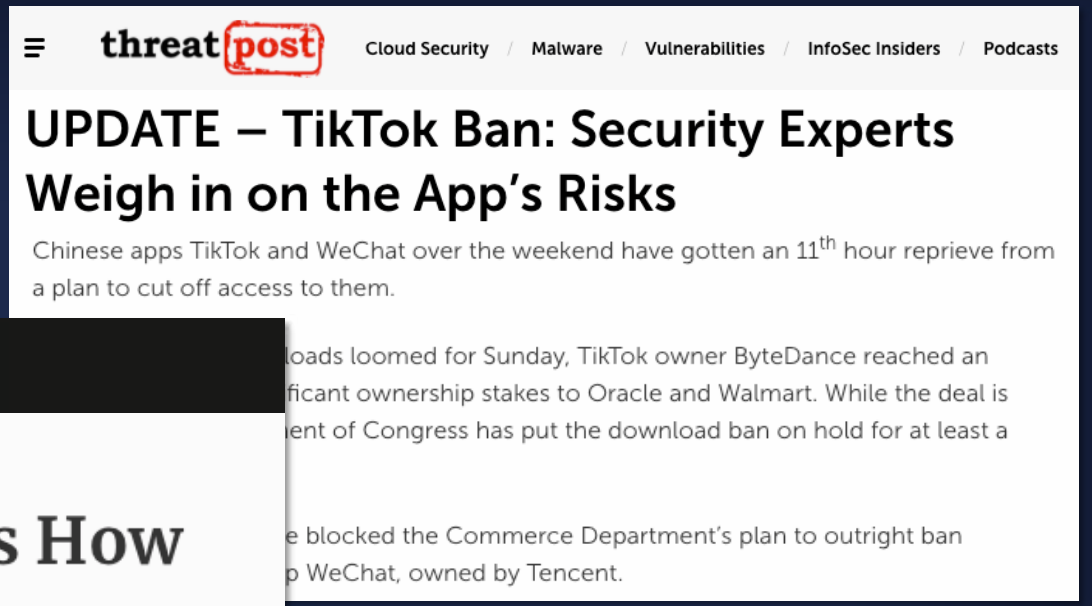
eSENTIRE

Cyber risk has become an issue of fiduciary care

Yet cyber risk is not consider material or covered as part of IT assessments

eSENTIRE

Businesses feel the aftershocks of Geo-political tectonic events



threatpost

Cloud Security / Malware / Vulnerabilities / InfoSec Insiders / Podcasts

UPDATE – TikTok Ban: Security Experts Weigh in on the App's Risks

Chinese apps TikTok and WeChat over the weekend have gotten an 11th hour reprieve from a plan to cut off access to them.

loads loomed for Sunday, TikTok owner ByteDance reached an ficant ownership stakes to Oracle and Walmart. While the deal is ent of Congress has put the download ban on hold for at least a

e blocked the Commerce Department's plan to outright ban p WeChat, owned by Tencent.

Forbes

Is TikTok Raiding Your Privacy In 2020? Here Is How To Stop It

Privacy is dead; long live privacy. The hope in that phrase is that the constant barrage against privacy by social media companies, and the internet in general, will never be as complete as privacy advocates fear. The short video phenom, TikTok, is stirring that fear anew. This post will tell you how to lock it down as much as possible.

eSENTIRE

ACCOUNTABILITY

COMPLIANCE + CONTRACTS + COVERAGE

ACCESS

REMOTE WORKERS

ASSETS

CLOUD-BASES

WORKLOADS

DISTRIBUTED

HANDS-ON

KEYBOARD

MALWARE

AS-A-SERVICE

CULTURAL

ENGINEERING

EMERGING

TECHNOLOGY

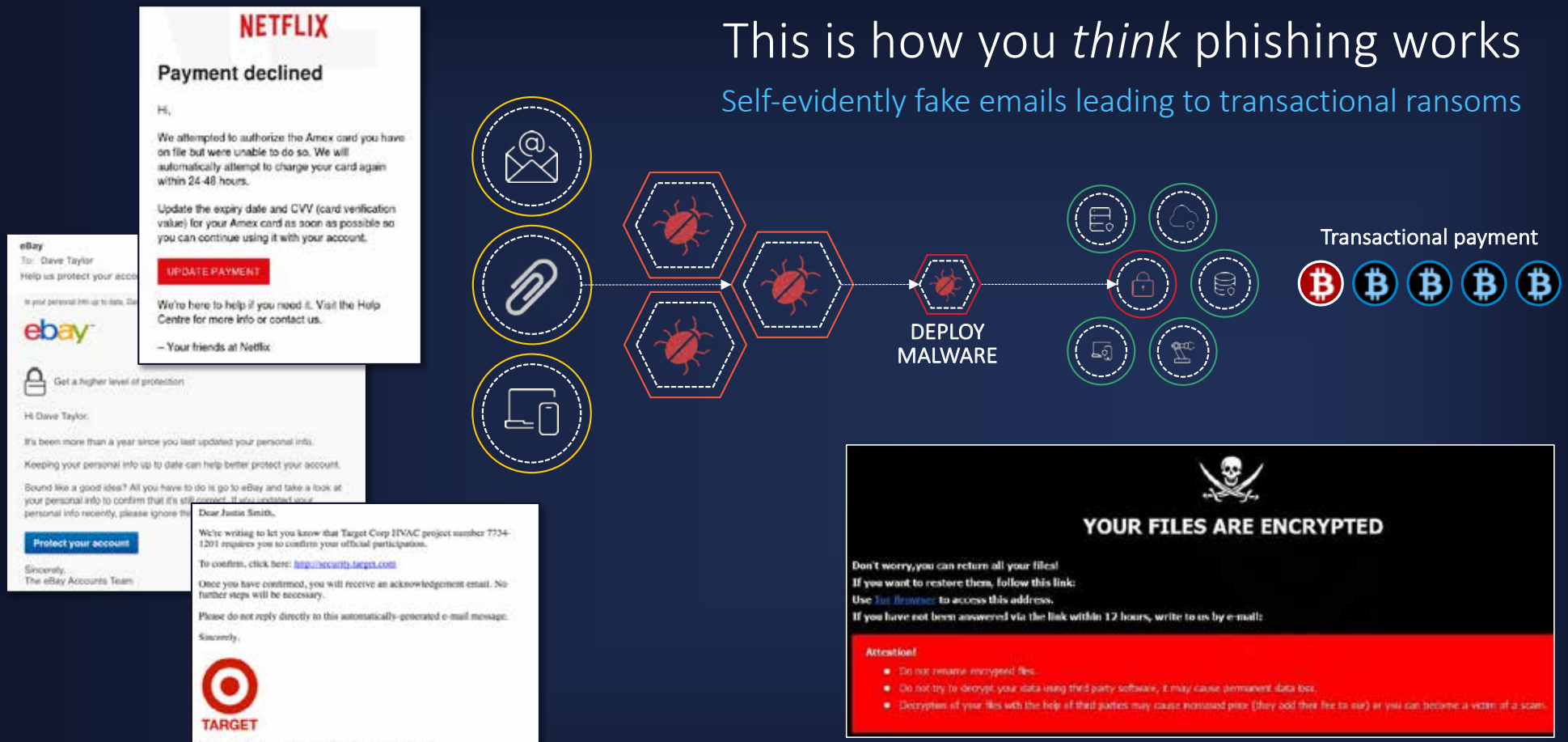
SOPHISTICATED

THREATS

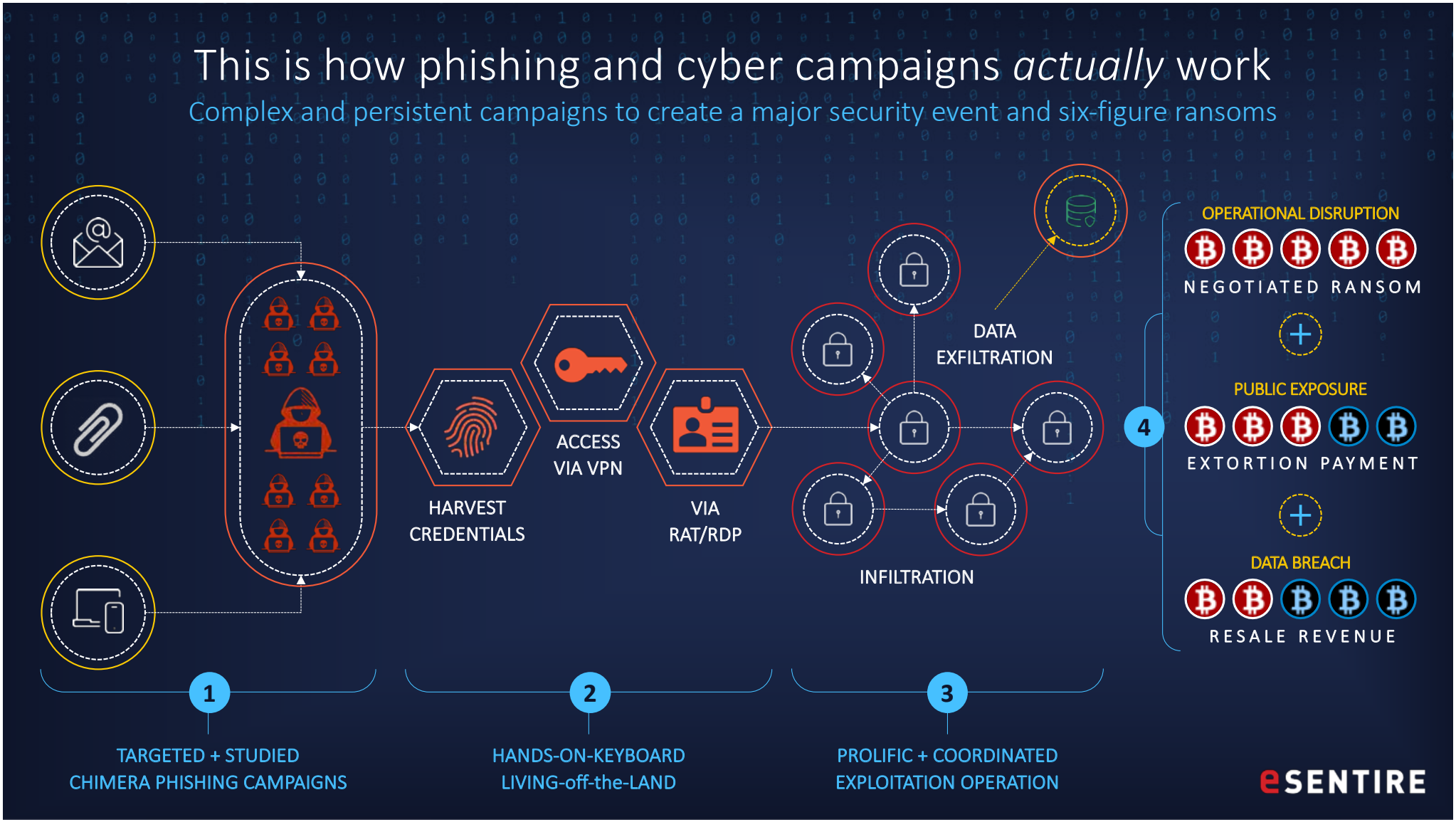
eSENTIRE

This is how you *think* phishing works

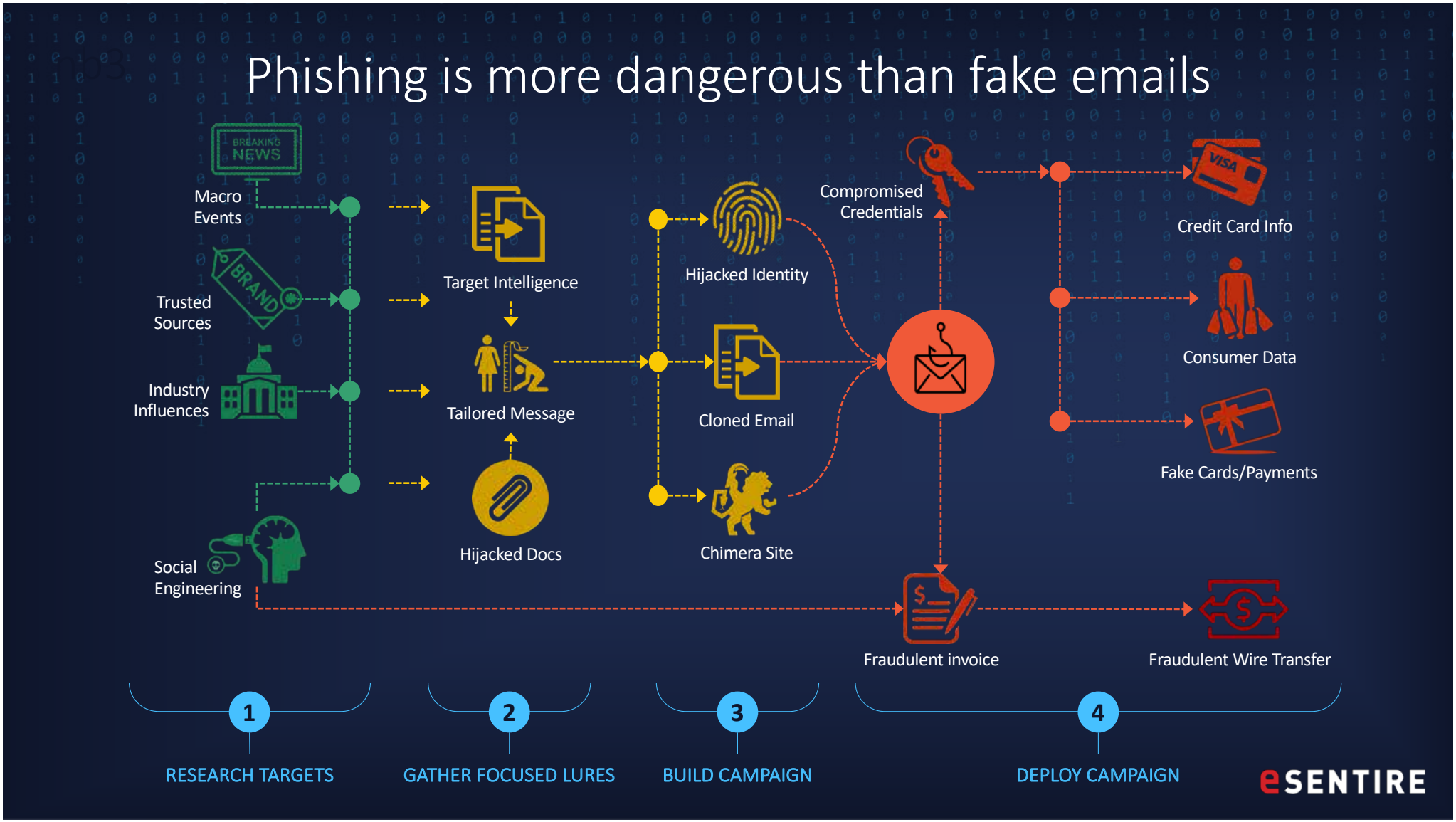
Self-evidently fake emails leading to transactional ransoms



eSENTIRE

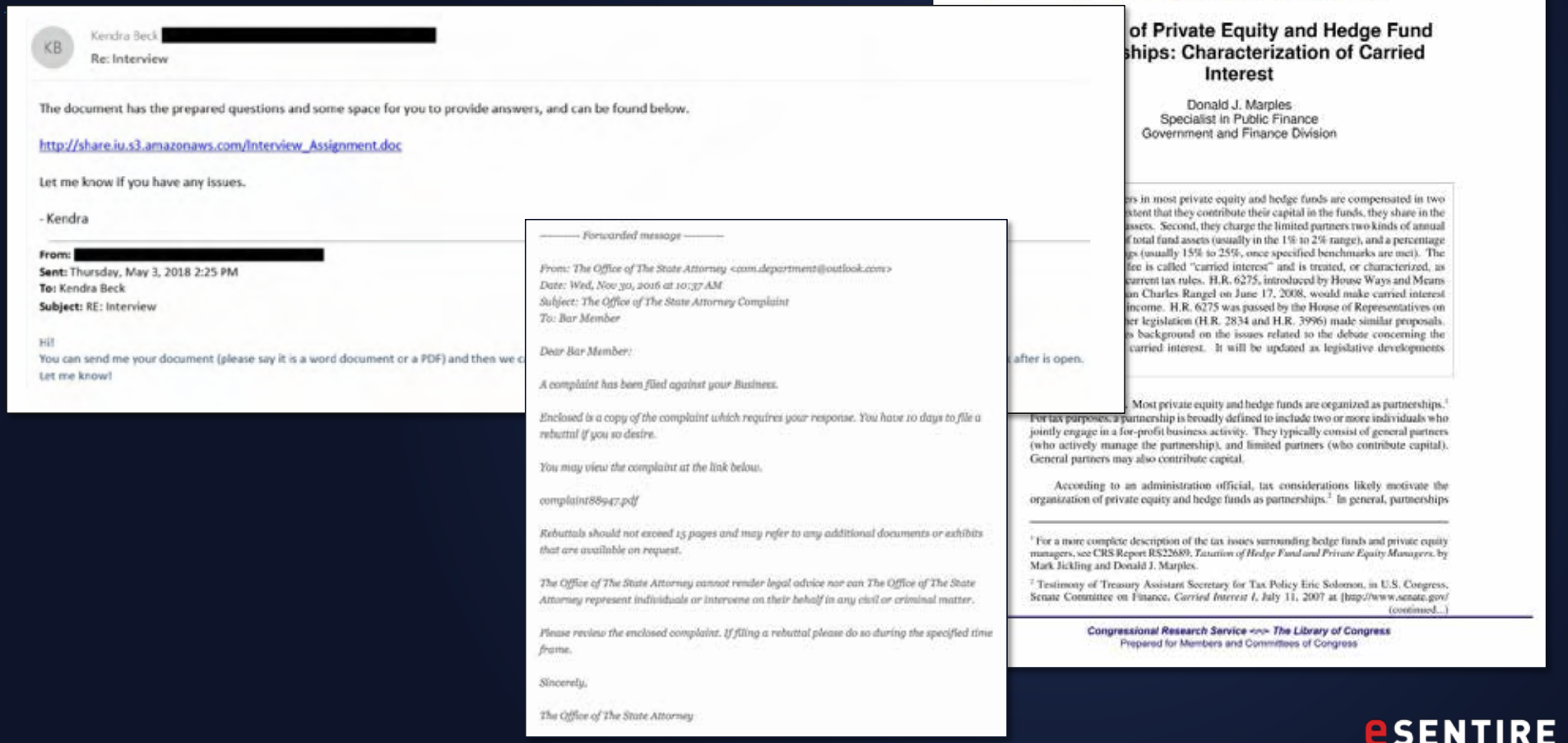

This is how phishing and cyber campaigns *actually* work
Complex and persistent campaigns to create a major security event and six-figure ransoms
HARVEST CREDENTIALS
ACCESS VIA VPN
VIA RAT/RDP
INFILTRATION
DATA EXFILTRATION
4
OPERATIONAL DISRUPTION
NEGOTIATED RANSOM
PUBLIC EXPOSURE
EXTORTION PAYMENT
DATA BREACH
RESALE REVENUE
1
TARGETED + STUDIED
CHIMERA PHISHING CAMPAIGNS
2
HANDS-ON-KEYBOARD
LIVING-off-the-LAND
3
PROLIFIC + COORDINATED
EXPLOITATION OPERATION
eSENTIRE

Phishing is more dangerous than fake emails



They understand your business

Exploiting industry culture to mimic trusted actors



Kendra Beck [redacted]
Re: Interview

The document has the prepared questions and some space for you to provide answers, and can be found below.

http://share.iu.s3.amazonaws.com/Interview_Assignment.doc

Let me know if you have any issues.

- Kendra

From: [redacted]
Sent: Thursday, May 3, 2018 2:25 PM
To: Kendra Beck
Subject: RE: Interview

Hi!
You can send me your document (please say it is a word document or a PDF) and then we c
Let me know!

after is open.

———— Forwarded message ————

From: The Office of The State Attorney <com.department@outlook.com>
Date: Wed, Nov 30, 2016 at 10:37 AM
Subject: The Office of The State Attorney Complaint
To: Bar Member

Dear Bar Member:

A complaint has been filed against your Business.

Enclosed is a copy of the complaint which requires your response. You have 10 days to file a rebuttal if you so desire.

You may view the complaint at the link below.

complaint88947.pdf

Rebuttals should not exceed 15 pages and may refer to any additional documents or exhibits that are available on request.

The Office of The State Attorney cannot render legal advice nor can The Office of The State Attorney represent individuals or intervene on their behalf in any civil or criminal matter.

Please review the enclosed complaint. If filing a rebuttal please do so during the specified time frame.

Sincerely,

The Office of The State Attorney

Order Code RS22717

CRS Report for Congress

of Private Equity and Hedge Fund
ships: Characterization of Carried Interest

Donald J. Marples
Specialist in Public Finance
Government and Finance Division

ers in most private equity and hedge funds are compensated in two
xtent that they contribute their capital in the funds, they share in the
ssets. Second, they charge the limited partners two kinds of annual
f total fund assets (usually in the 1% to 2% range), and a percentage
gs (usually 15% to 25%, once specified benchmarks are met). The
fee is called "carried interest" and is treated, or characterized, as
current tax rules. H.R. 6275, introduced by House Ways and Means
an Charles Rangel on June 17, 2008, would make carried interest
income. H.R. 6275 was passed by the House of Representatives on
her legislation (H.R. 2834 and H.R. 3996) made similar proposals.
s background on the issues related to the debate concerning the
carried interest. It will be updated as legislative developments

. Most private equity and hedge funds are organized as partnerships.[1] For tax purposes, a partnership is broadly defined to include two or more individuals who jointly engage in a for-profit business activity. They typically consist of general partners (who actively manage the partnership), and limited partners (who contribute capital). General partners may also contribute capital.

According to an administration official, tax considerations likely motivate the organization of private equity and hedge funds as partnerships.[2] In general, partnerships

[1] For a more complete description of the tax issues surrounding hedge funds and private equity managers, see CRS Report RS22689, *Taxation of Hedge Fund and Private Equity Managers*, by Mark Jickling and Donald J. Marples.

[2] Testimony of Treasury Assistant Secretary for Tax Policy Eric Solomon, in U.S. Congress, Senate Committee on Finance, *Carried Interest I*, July 11, 2007 at [http://www.senate.gov/ (continued...)

Congressional Research Service <•> The Library of Congress
Prepared for Members and Committees of Congress

eSENTIRE

STATE-SPONSORED actors move down stream while ORGANIZED CRIME grows in ferocity and coordination

1

USING YOUR OWN TOOLS

HAND-ON-KEYBOARD

2

CRIMINAL ECONOMY

MALWARE AS-A-SERVICE

3

THEY UNDERSTAND YOUR BUSINESS

CULTURE-BASED ATTACKS

eSENTIRE

Attacks have dramatically increased in 2020

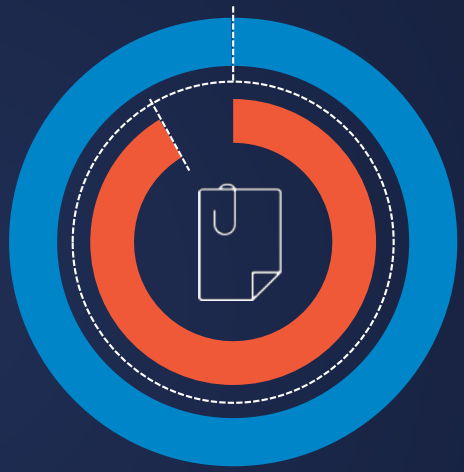
90%
Increase
IN ATTACKS

54%
Involve
EMAIL / PHISHING

130%
Increase
IN PAYMENTS

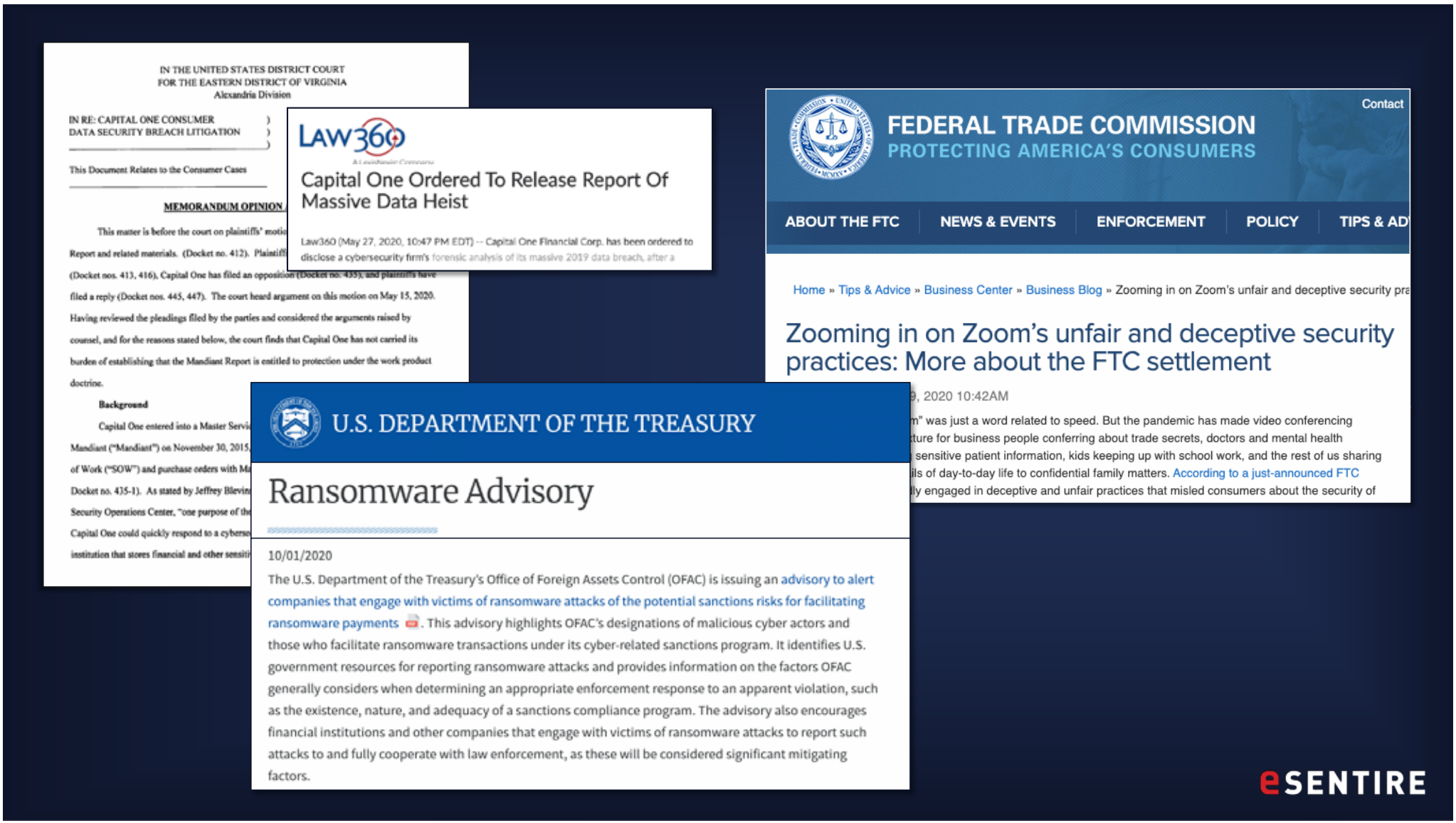
90%
Claim Increase
RANSOMWARE

216%
Increase
IN FUNDS DEFRAUDED



90%
Claim Increase
FRAUDULENT INVOICES

eSENTIRE


IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division
IN RE: CAPITAL ONE CONSUMER DATA SECURITY BREACH LITIGATION
This Document Relates to the Consumer Cases
MEMORANDUM OPINION
This matter is before the court on plaintiffs' motio
Report and related materials. (Docket no. 412). Plaintiff
(Docket nos. 413, 416), Capital One has filed an opposition (Docket no. 435), and plaintiffs have
filed a reply (Docket nos. 445, 447). The court heard argument on this motion on May 15, 2020.
Having reviewed the pleadings filed by the parties and considered the arguments raised by
counsel, and for the reasons stated below, the court finds that Capital One has not carried its
burden of establishing that the Mandiant Report is entitled to protection under the work product
doctrine.
Background
Capital One entered into a Master Servi
Mandiant ("Mandiant") on November 30, 2015,
of Work ("SOW") and purchase orders with Ma
Docket no. 435-1). As stated by Jeffrey Blevin
Security Operations Center, "one purpose of th
Capital One could quickly respond to a cyberse
institution that stores financial and other sensiti
LAW360
Capital One Ordered To Release Report Of Massive Data Heist
Law360 (May 27, 2020, 10:47 PM EDT) -- Capital One Financial Corp. has been ordered to disclose a cybersecurity firm's forensic analysis of its massive 2019 data breach, after a
U.S. DEPARTMENT OF THE TREASURY
Ransomware Advisory
10/01/2020
The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing an advisory to alert companies that engage with victims of ransomware attacks of the potential sanctions risks for facilitating ransomware payments. This advisory highlights OFAC's designations of malicious cyber actors and those who facilitate ransomware transactions under its cyber-related sanctions program. It identifies U.S. government resources for reporting ransomware attacks and provides information on the factors OFAC generally considers when determining an appropriate enforcement response to an apparent violation, such as the existence, nature, and adequacy of a sanctions compliance program. The advisory also encourages financial institutions and other companies that engage with victims of ransomware attacks to report such attacks to and fully cooperate with law enforcement, as these will be considered significant mitigating factors.
Contact
FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS
ABOUT THE FTC
NEWS & EVENTS
ENFORCEMENT
POLICY
TIPS & AD
Home » Tips & Advice » Business Center » Business Blog » Zooming in on Zoom's unfair and deceptive security pra
Zooming in on Zoom's unfair and deceptive security practices: More about the FTC settlement
9, 2020 10:42AM
n" was just a word related to speed. But the pandemic has made video conferencing
ture for business people conferring about trade secrets, doctors and mental health
sensitive patient information, kids keeping up with school work, and the rest of us sharing
ils of day-to-day life to confidential family matters. According to a just-announced FTC
ly engaged in deceptive and unfair practices that misled consumers about the security of
eSENTIRE

Cybersecurity is not an **IT Problem** to solve...
It's a **Business Risk** to manage.

GLOBAL
cyber risk

EXECUTION
cyber risk

DEAL VALUE
cyber risk

INTEGRATION
cyber risk

FUTURE DEALS
cyber risk

eSENTIRE

Cyber risk 5 pillar toolkit

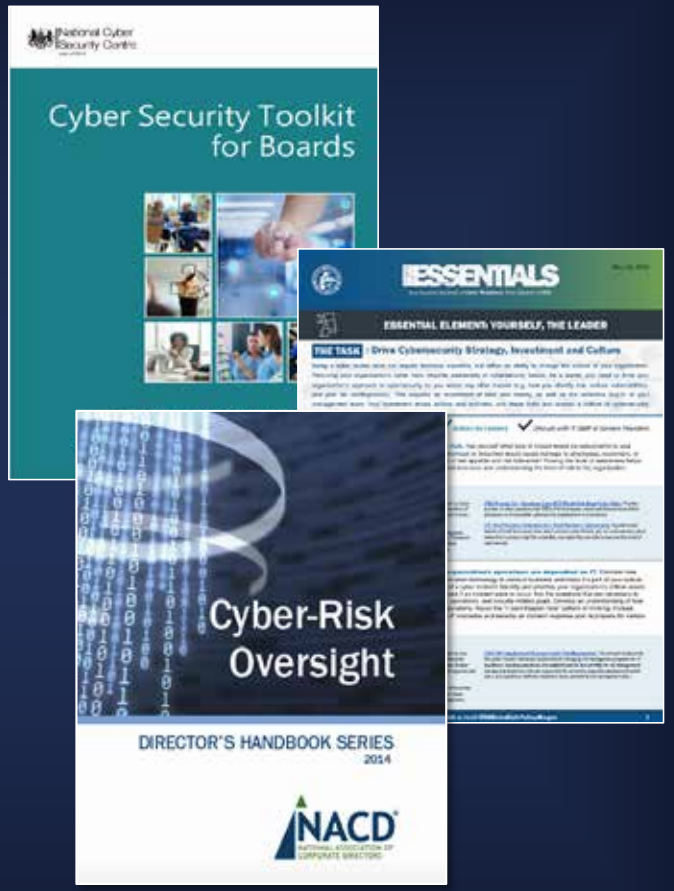
1 AWARENESS
Understand the impact of cyber risks and trends, experiencing business impact of a breach and exposing personal risks

2 RISK
Identifying non-public assets, protected data, and documenting regulatory and contractual obligations

3 PROGRAM
Establishing budget, staffing and programs that align to overall business risk priorities

4 REPORTING
Annual planning, quarterly reporting, dashboards and peer/industry comparisons of performance

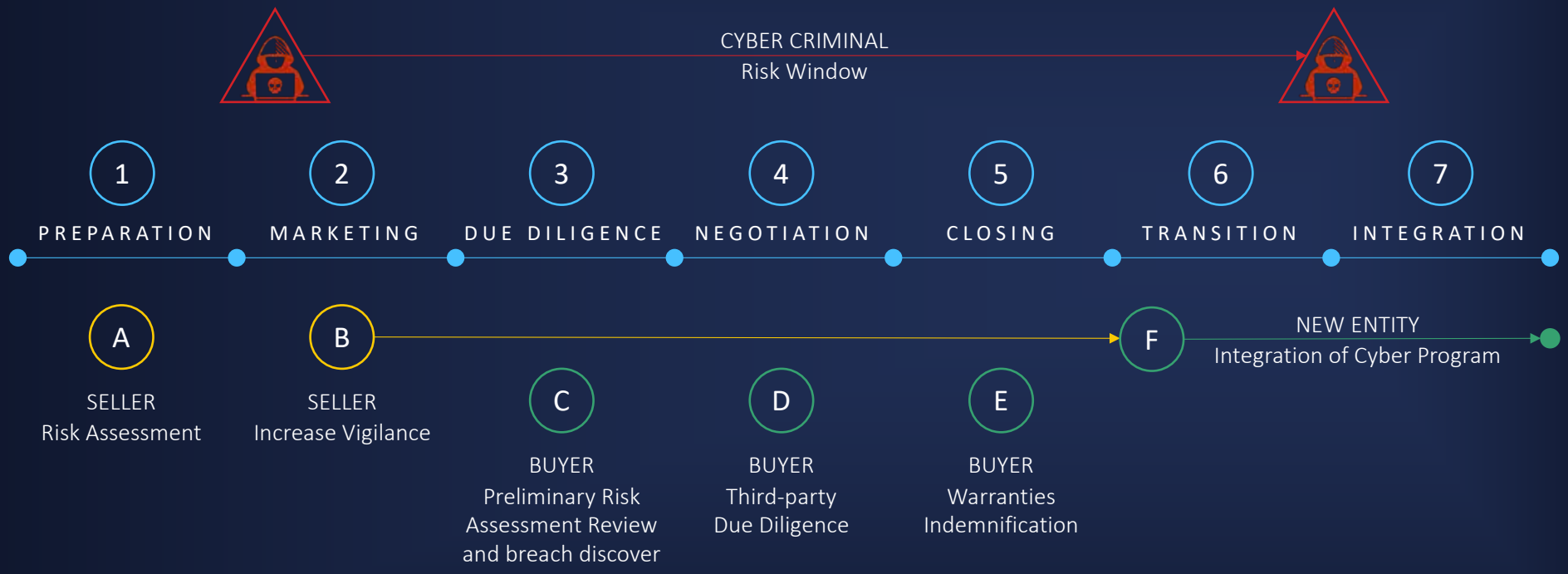
5 INCIDENTS
Understanding incident response, board roles, critical business decisions, reporting to authorities and crisis communications



eSENTIRE

65% of firms expressed buyer's remorse due to cybersecurity issues

Only 36% felt that they had adequate time and resources to assess cyber risk



https://techcrunch.com/2020/09/10/its-time-to-better-identify-the-cost-of-cybersecurity-risks-in-ma-deals/

eSENTIRE

Examine cyber risks associated with the seller

Risk + obligation awareness, risk assessment, posture, reporting and incident response

1. **INVENTORY PROTECTED + NON-PUBLIC ASSETS**
   PII, PCI/financial, healthcare, protected, intellectual property
2. **AUDIT PRIVACY + SECURITY OBLIGATIONS**
   Regulatory compliance, privacy laws, contractual obligations
3. **ASSESS INDUSTRY-BASED RISK**
   Top threat vectors, public breaches, regulatory disclosures
4. **EXAMINE BREACH + SECURITY EVENT DISCLOSURES**
   Regulatory declarations, breaches, fines and corrective actions
5. **EVALUATE SELLER'S CYBER POSTURE**
   Awareness, risk assessments, programs + budget, reporting
6. **ASSESS RESIDUAL RISK GAPS**
   Risk registry, insurance coverage, security vendors
7. **ASSESS SUPPLY CHAIN RISK**
   Policies + procedures, security measures, shared risk
8. **EXAMINE PRODUCT (APP DEV) RISK**
   DevOps security programs, third-party assessments
9. **PLAN SELLER INTEGRATION INTO BUYER PROGRAM**
   Integration plan, insurance coverage, outsourcing support
10. **DETERMINE WARRANTIES + INDEMNITIES**
    Min. security requirements, warranties, notifications, coverage

eSENTIRE

A SECTION A
CYBERSECURITY GOVERNANCE

1 CYBERSECURITY LEADERSHIP

1.A Chief information security officer (CISO/CSO)

1.B Cybersecurity governance committee (CSG)

1.C Documented cybersecurity roles and responsibilities

1.D Documented cybersecurity risk profile and registry

1.E Documented cybersecurity program

1.F Documented business continuity plan (BCP)

1.G Documented incident response (IR) plan

2 CLASSIFICATION AND INVENTORY OF ASSETS

2.A Personal data/identifiable info (PD/PII)

2.B Financial data, accounts and transaction information

2.C Client account and transaction records

2.D Confidential health or employee records

2.E Identify sensitive intellectual property

3 MAP REGULATORY REQUIREMENTS

3.A Federal regulations (HIPAA, GLBA)

3.B Privacy regulations (GDPR, CCPA)

3.C Map of jurisdictions in which firms/clients operate

3.D Map of federal statutes

3.E Map of state statutes

4 CYBER INSURANCE

4.A Documented policy and carrier

4.B Documented minimum security standards

4.C Documented notification of claim procedures

eSENTIRE

B SECTION B
RISK ASSESSMENT

5 RISK PROFILE

5.A Document industry associated risks

5.B Evaluate likelihood and consequences

5.C Create a risk registry

5.D Monitor risk mitigation activities and performance

6 ANNUAL RISK ASSESSMENT

6.A Document known threat actors and persistent threats

6.B Document technology base vulnerabilities

6.C Document business model vulnerabilities

6.D Document regulatory obligations and penalties

6.E Document client obligations and penalties

6.F Document supply chain obligations and penalties

7 ANNUAL PENETRATION TEST

7.A Conduct annual penetration test

7.B Document identified vulnerabilities and recommendations

7.C Document identified compliance violations

8 PERIODIC AD HOC ASSESSMENT

8.A Review security controls given material change

8.B Document risks associated with material change

8.C Document required changes to policies and insurance

C SECTION C
SECURITY PROGRAM

9 ASSET INVENTORY AND DEVIC MANAGEMENT

9.A Documented operating systems, versions and mapping

9.B Mapped network mapping, file structure and segments

9.C Documented security controls and infrastructure

9.D Documented endpoints (MAC address, OS)

9.E Mapped cloud-based services and data

9.F List of users, groups and privileges

10 ACCESS CONTROL TO SENSITIVE DATA+SYSTEMS

10.A Documented and controlled user credential standards

10.B Documented and controlled user privilege standards

10.C Multi-factor authentication

11 DATA ENCRYPTION + RENTENTION

11.A Controls and standards to encrypt storage devices

11.B Controls and standards to encrypt cloud devices

11.C Virtual private network (VPN) controls

11.D Documented data retention standards

11.E Documented data destruction standards

eSENTIRE

C

SECTION C - CON'T
SECURITY PROGRAM

12 ICS / INDUSTRIAL CONTROLS / IIoT

12.A Discovery and control of workstations and devices

12.B Discovery of L2 devices (PLCs and controllers)

12.C Mapped industrial controls and intersections with IT

12.D Documented controls to update and maintain ICS systems

13 MOBILE DEVICES

13.A Mobile device management (MDM)

13.B Endpoint prevention or next-generation antivirus (NGAV)

13.C Endpoint detection and response (EDR)

14 BACK-UP + RECOVERY

14.A Documented back-up and recovery services

14.B Documented testing procedures

15.0 Application Testing and Maintenance

15.A Documented controls to test new applications

15.B Documented controls to update applications

15.C Documented controls to verify application status

15 APPLICATION TESTING + MAINTENANCE

15.A Documented controls to test new applications

15.B Documented controls to update applications

15.C Documented controls to verify application status

16 CONTINUOUS MONITORING FOR UNAUTHORIZED ACCESS

16.A Security monitoring and logging

16.B Proactive threat hunting

17 PEOPLE + TRAINING

17.0 People and Training

17.A Documented annual security awareness training

17.B Documented phishing testing

17.C Documented red-team blue-team exercises

eSENTIRE

B

SECTION D
SUPPLY CHAIN RISK MANAGEMENT

18 RISK PROFILE

18.A Documented supply chain risk management policy

18.B Documented procedures to evaluate vendors

18.C Documented minimum security standards for vendors

18.D Documented security event notification for vendors

18.E Documented warranties, requirements and liability clauses

C

SECTION E
INCIDENT RESPONSE

19 ASSET INVENTORY AND DEVIC MANAGEMENT

19.A Documented and tested incident response plan

19.B Documented team roles and responsibilities

19.C Documented procedures for the collection of forensics

19.D Documented reporting mechanisms and procedures

19.E Documented notification procedures

19.F Documented review and lessons learned procedures

eSENTIRE

The Three-P's of mitigating third-party risk

Policies + Prevention + Promises

1 POLICIES

MEASURE

REQUIREMENTS
Needs analysis, business case and gated approvals

SELECTION
Risk measurement tools including due diligence assessments, and evaluation process

CONTROLS
Minimum security controls and transparent disclosures

CONTRACTS
Obligations, min. security standards, notifications, warranties and indemnificaiton

2 PREVENTION

MINIMIZE

ASSETS
Identify sensitive assets and data

OBLIGATIONS
Identify legal, contractual and regulatory obligations

RISK
Define risk appetite, conduct risk assessment and minimize residual risk

DEFEND
Define defensive requirements and allocate resources

3 PROMISES

MITIGATE

OBLGATIONS
Identify legal, contractual and regulatory obligations

DEMARK RESPONSIBILITIES
Service definitions and division of duties,

MINIMUM STANDARDS
Security programs, testing and reporting

NOTIFICATIONS
Trigger and definitions, attestations, regulatory compliance

WARRANTIES
Insurance, shared costs and efforts, financial penalties

eSENTIRE

Cybersecurity is not an **IT Problem** to solve...
It's a **Business Risk** to manage.

ENGAGE
early in the deal

QUANTIFY
Liability and risk

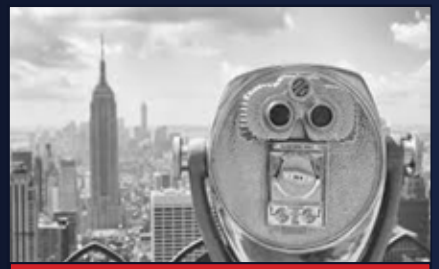
UNDERSTAND
the implications of Due Diligence

FACTOR
cyber risk into the negotiations

TRANSFER
liability through Insurance

eSENTIRE

Public references



Department of Financial Services

NYCRR 500 Section 11

AITEC

AIMA

National Cyber Security Centre

a part of GCHQ

Supply Chain Security Guidance

eSENTIRE

COVID-19: Learn from past to invest in the future

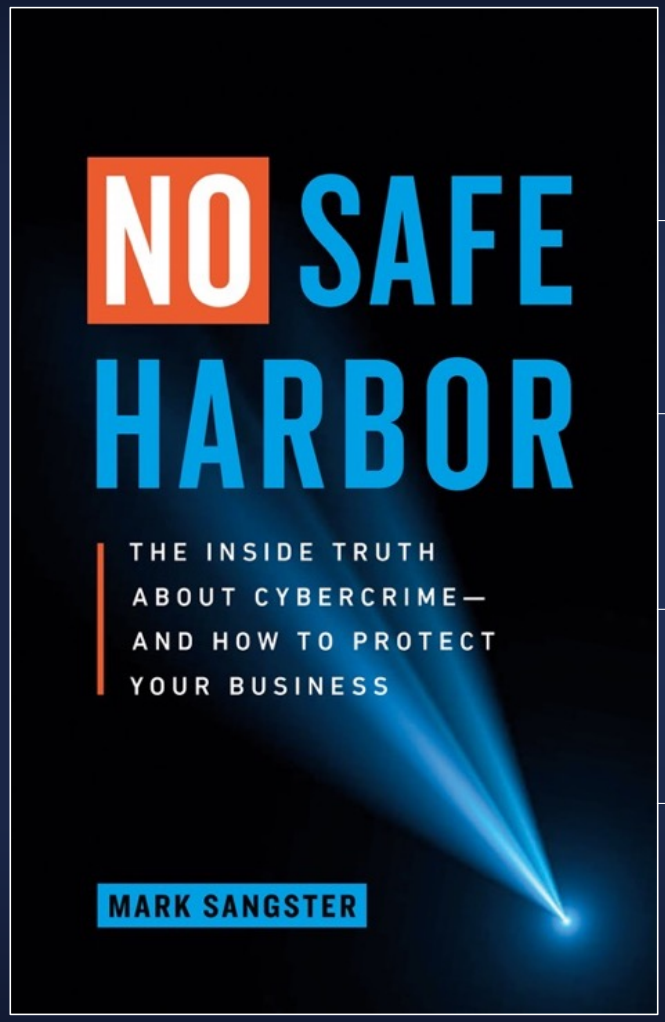
1997 1998 1999 2000 **2001** 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 **2012** 2013 2014 2015 2016 2017 2018 2019 **2020** 2021 2022 2023

eSENTIRE

Mark Sangster

Principal Evangelist and VP
Industry Security Strategies

mark.sangster@esentire.com
@mbsangster
Linkedin.com/in/mbsangster
@cyber_mbsangster
mbsangster.com/book



1. **Expertise beats headcount**
   Your skills must match your expanding ecosystem.
2. **Gap exists at all levels**
   Gaps go beyond the IT team to include employees and C-suite
3. **Evaluate the systemic issues**
   It's easy to blame the people but that rarely solves the real problems
4. **Security equals business risk**
   Cybersecurity program must reach all levels of the business

eSENTIRE