PROGRAM MATERIALS
Program #3133
January 22, 2021

Targeting Law Firms: Inside the Cyber Criminal Economy

Celesq® AttorneysEd Center
www.celesq.com

5255 North Federal Highway, Suite 100, Boca Raton, FL 33487
Phone 561-241-1919

Targeting Law Firms

Inside the Cyber Criminal Economy

Celesq Attorneys Education Center| 22 JAN 2021

Mark Sangster

Principal Evangelist and VP industry Security Strategies

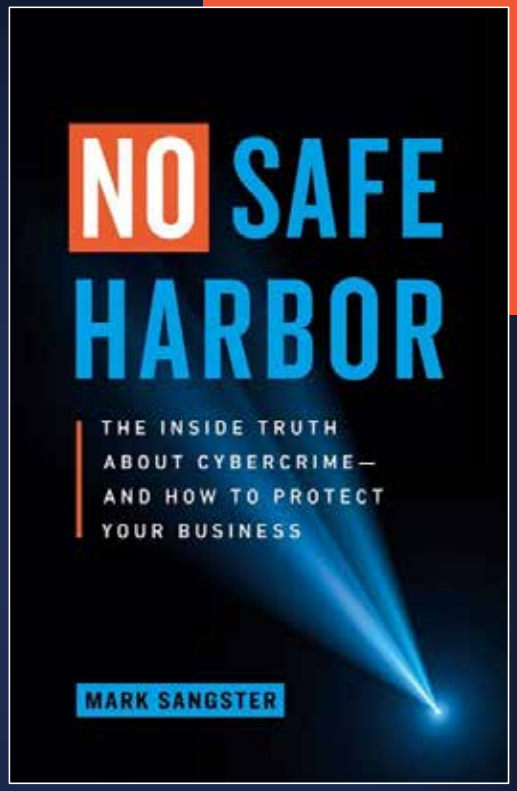
mark.sangster@esentire.com

@mbsangster

@cyber_mbsangster

Linkedin.com/in/mbsangster

mbsangster.com/book



eSENTIRE

Security Experts In Legal Services

6	75+	1K+	20+	2021
YEARS ILTA + LS-ISAO	LEADERSHIP Workshops	LAW STAFF Trained	LAW SECURITY Resources	ILTA Programs

International Legal Technology Association
ILTACON
LegalSEC
ALA Association of Legal Administrators
ABA
HARVARD LAW SCHOOL
LEGAL SERVICES ISAO
ALM Legaltech

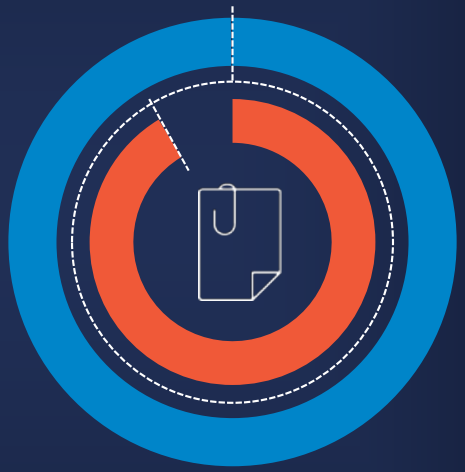
Phishing + Ransomware + Business Email Compromise

90% Increase IN ATTACKS

130% Increase IN PAYMENTS

54% Involve EMAIL / PHISHING

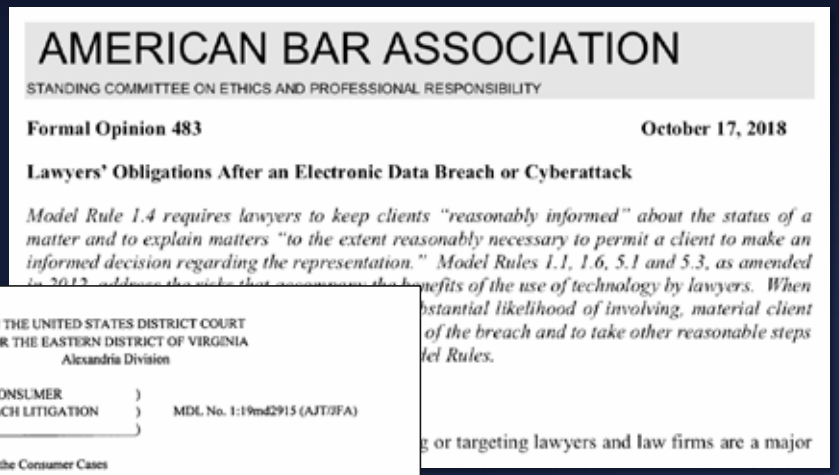
216% Increase IN FUNDS DEFRAUDED



90% Claim Increase FRAUDULENT INVOICES

eSENTIRE

Legal + ethical obligations



AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483 **October 17, 2018**

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

Model Rule 1.4 requires lawyers to keep clients "reasonably informed" about the status of a matter and to explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation." Model Rules 1.1, 1.6, 5.1 and 5.3, as amended

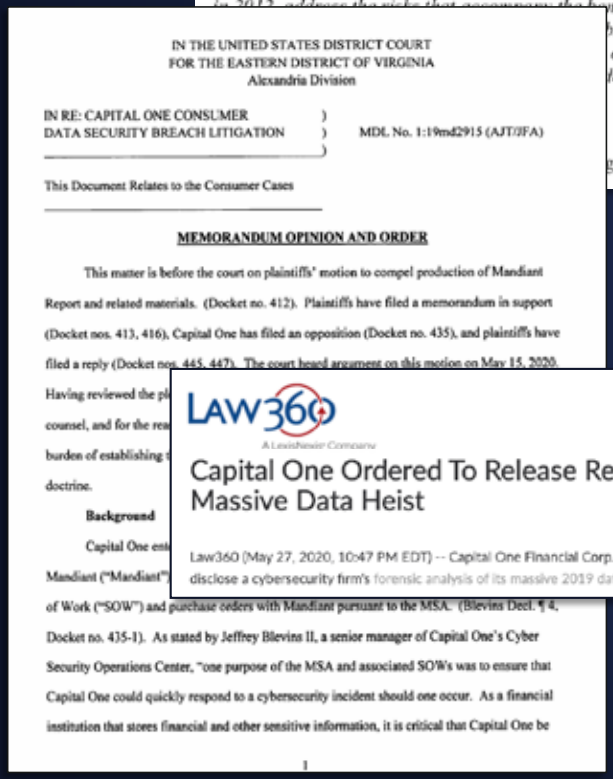
benefits of the use of technology by lawyers. When

bstantial likelihood of involving, material client

of the breach and to take other reasonable steps

del Rules.

g or targeting lawyers and law firms are a major



IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN RE: CAPITAL ONE CONSUMER DATA SECURITY BREACH LITIGATION) MDL No. 1:19md2915 (AJT/JFA)

This Document Relates to the Consumer Cases

MEMORANDUM OPINION AND ORDER

This matter is before the court on plaintiffs' motion to compel production of Mandiant Report and related materials. (Docket no. 412). Plaintiffs have filed a memorandum in support (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 pl
counsel, and for the rea
burden of establishing
doctrine.

Background

Capital One ent
Mandiant ("Mandiant"
of Work ("SOW") and purchase orders with Mandiant pursuant to the MSA. (Blevins Decl. ¶ 4, Docket no. 435-1). As stated by Jeffrey Blevins II, a senior manager of Capital One's Cyber Security Operations Center, "one purpose of the MSA and associated SOW's was to ensure that Capital One could quickly respond to a cybersecurity incident should one occur. As a financial institution that stores financial and other sensitive information, it is critical that Capital One be

1

LAW360

A LexisNexis Company

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

Contact

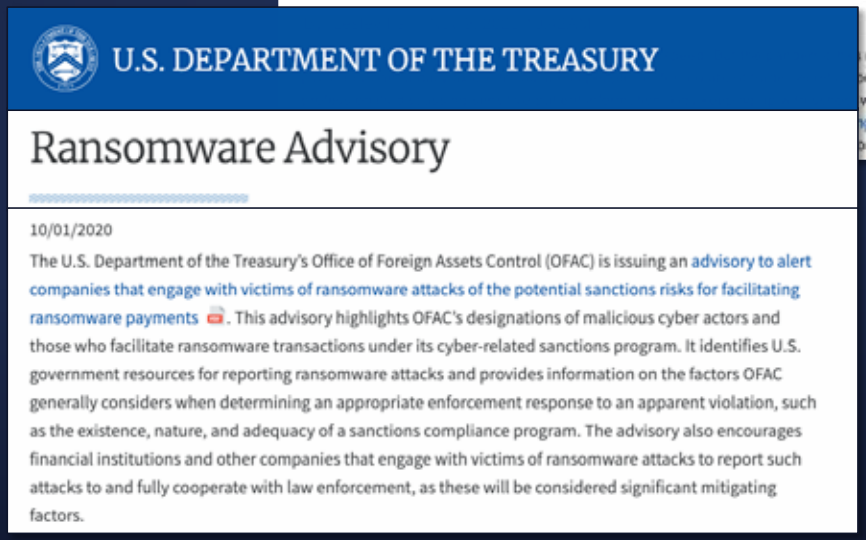
FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

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

made video conferencing
ctors and mental health
work, and the rest of us sharing
g to a just-announced FTC
nsumers about the security of



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.

eSENTIRE

Global cybercrime losses well over $1 Trillion

Sarah Coble News Writer

info security
STRATEGY | INSIGHT | TECHNOLOGY

Global losses from cybercrime now total over $1tn, according to a new report released today by McAfee in partnership with the Center for Strategic and International Studies (CSIS).

"The Hidden Costs of Cybercrime" concludes that cybercrime costs the world economy more than one percent of global GDP. A 2018 study put global losses more than 50% lower, at around $600bn.

Independent technology market research specialist Vanson Bourne was commissioned by McAfee to undertake the research upon which the report is based. Between April and June 2020, researchers interviewed 1,500 IT and line-of-business decision makers.

Respondents came from Australia (200), Canada (200), France (200), Germany (200), Japan (200), the UK (200), and the US (300).

The report focuses not just on the significant financial cost of cybercrime but also on its wider impact on things like company performance and brand reputation. Nearly all (92%) companies surveyed reported feeling effects from cybercrime that went beyond monetary losses.

Over a third (33%) of survey respondents stated downtime caused by IT security incidents cost them between $100,000 and $500,000. The average cost to organizations from their longest amount of downtime in 2019 was $762,231.

eSENTIRE

Cybercrime is the world's third largest economy

DARKReading | SIGN UP FOR OUR NEWSLETTERS

Cybercrime May Be the World's Third-Largest Economy by 2021

The underground economy is undergoing an industrialization wave and booming like never before.

As organizations go digital, so does crime. Today, cybercrime is a massive business in its own right, and criminals everywhere are clamoring to get a piece of the action as companies and consumers invest trillions to stake their claim in the digital universe.

That's why the World Economic Forum's (WEF) "Global Risks Report 2020" states that cybercrime will be the second most-concerning risk for global commerce over the next decade until 2030. It's also the seventh most-likely risk to occur, and eighth most impactful. And the stakes have never been higher. Revenue, profits, and the brand reputations of enterprises are on the line; mission-critical infrastructure is being exposed to threats; and nation-states are engaging in cyber warfare and cyber espionage with each other.

Putting things into perspective: Walmart, which racks up America's greatest firm earnings, generated a mind-blowing $514 billion in revenue last year. Yet cybercrime earns 12 times that. Both sell a huge variety of products and services. In fact, in terms of earnings, cybercrime puts even Tesla, Facebook, Microsoft, Apple, Amazon, and Walmart to shame. Their combined annual revenue totals "just" $1.28 trillion.

#3 Economy

#2 Global Risk

Worth more than the combined revenues of

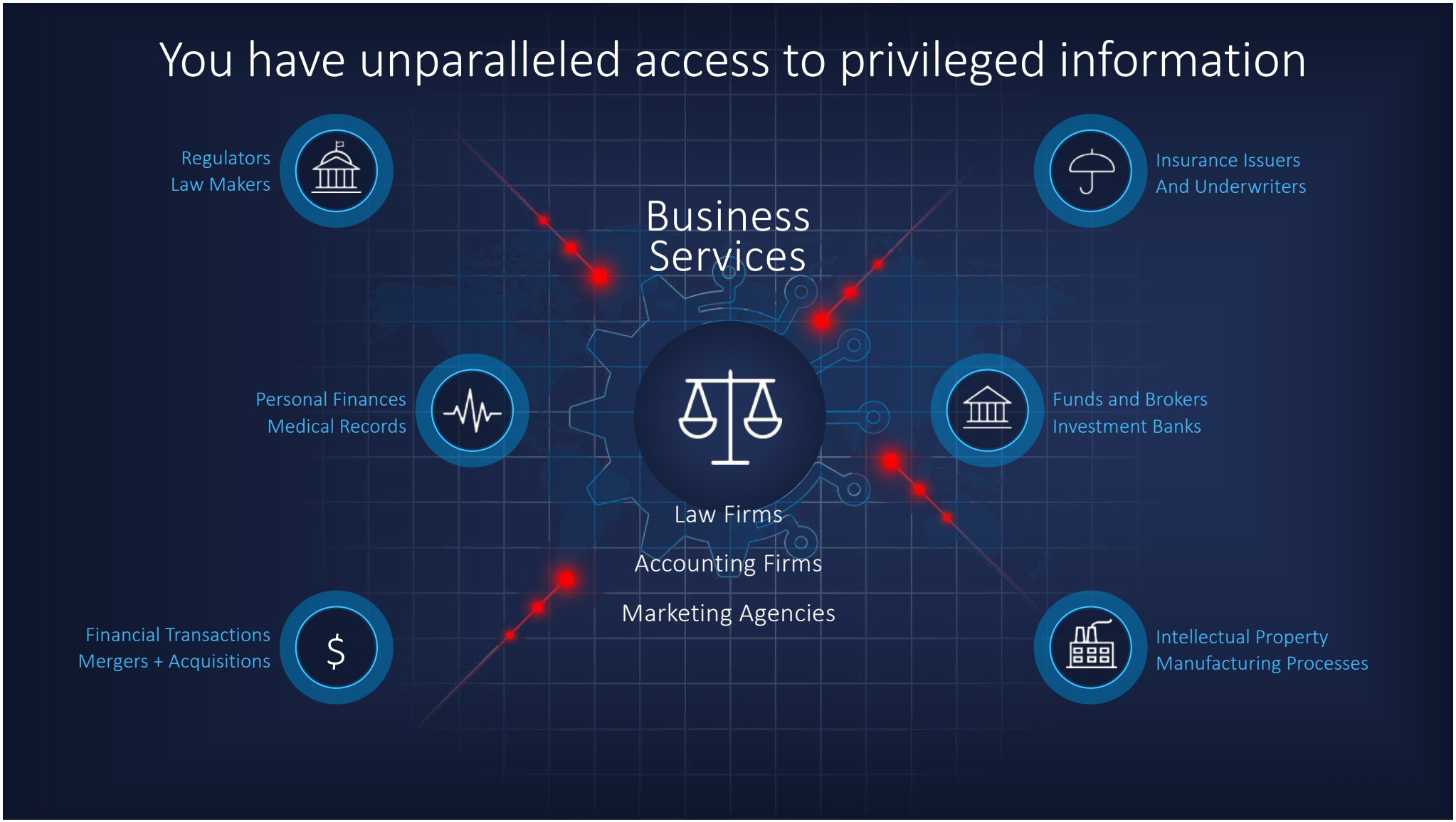
Walmart

TESLA

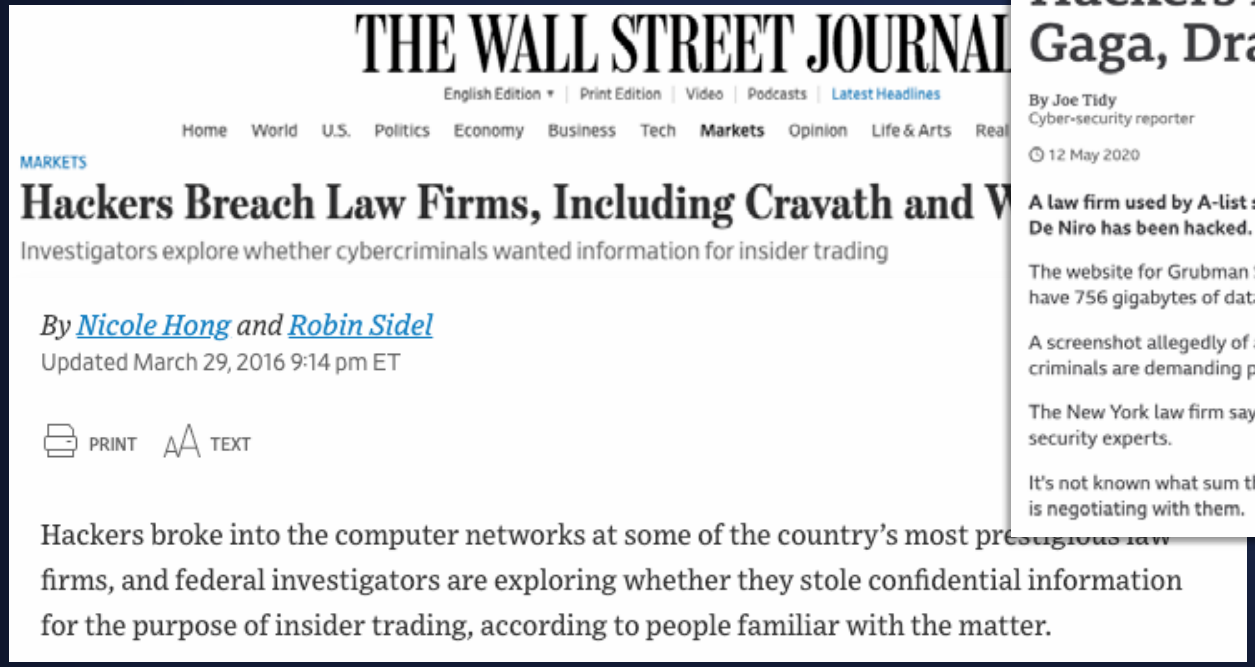
amazon

eSENTIRE

You have unparalleled access to privileged information



Law firms are a stepping stone in the criminal endgame



THE WALL STREET JOURNAL

English Edition ▾ | Print Edition | Video | Podcasts | Latest Headlines

Home World U.S. Politics Economy Business Tech **Markets** Opinion Life & Arts Real

MARKETS

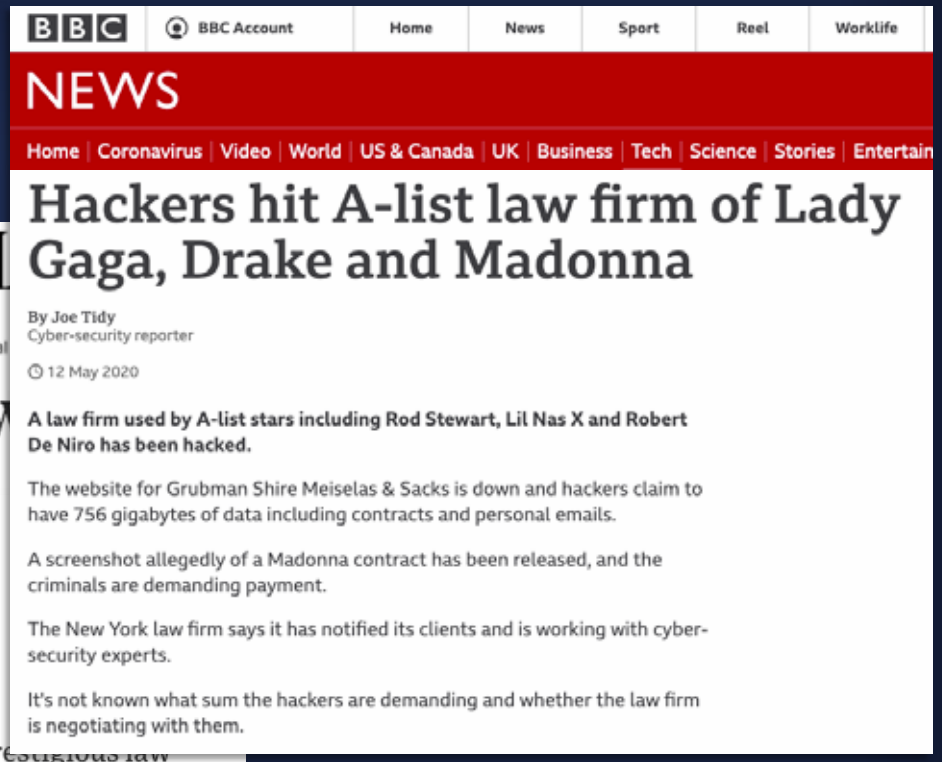
Hackers Breach Law Firms, Including Cravath and V

Investigators explore whether cybercriminals wanted information for insider trading

By Nicole Hong and Robin Sidel
Updated March 29, 2016 9:14 pm ET

PRINT TEXT

Hackers broke into the computer networks at some of the country's most prestigious law firms, and federal investigators are exploring whether they stole confidential information for the purpose of insider trading, according to people familiar with the matter.



BBC | BBC Account | Home | News | Sport | Reel | Worklife

NEWS

Home | Coronavirus | Video | World | US & Canada | UK | Business | Tech | Science | Stories | Entertain

Hackers hit A-list law firm of Lady Gaga, Drake and Madonna

By Joe Tidy
Cyber-security reporter

12 May 2020

A law firm used by A-list stars including Rod Stewart, Lil Nas X and Robert De Niro has been hacked.

The website for Grubman Shire Meiselas & Sacks is down and hackers claim to have 756 gigabytes of data including contracts and personal emails.

A screenshot allegedly of a Madonna contract has been released, and the criminals are demanding payment.

The New York law firm says it has notified its clients and is working with cyber-security experts.

It's not known what sum the hackers are demanding and whether the law firm is negotiating with them.

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

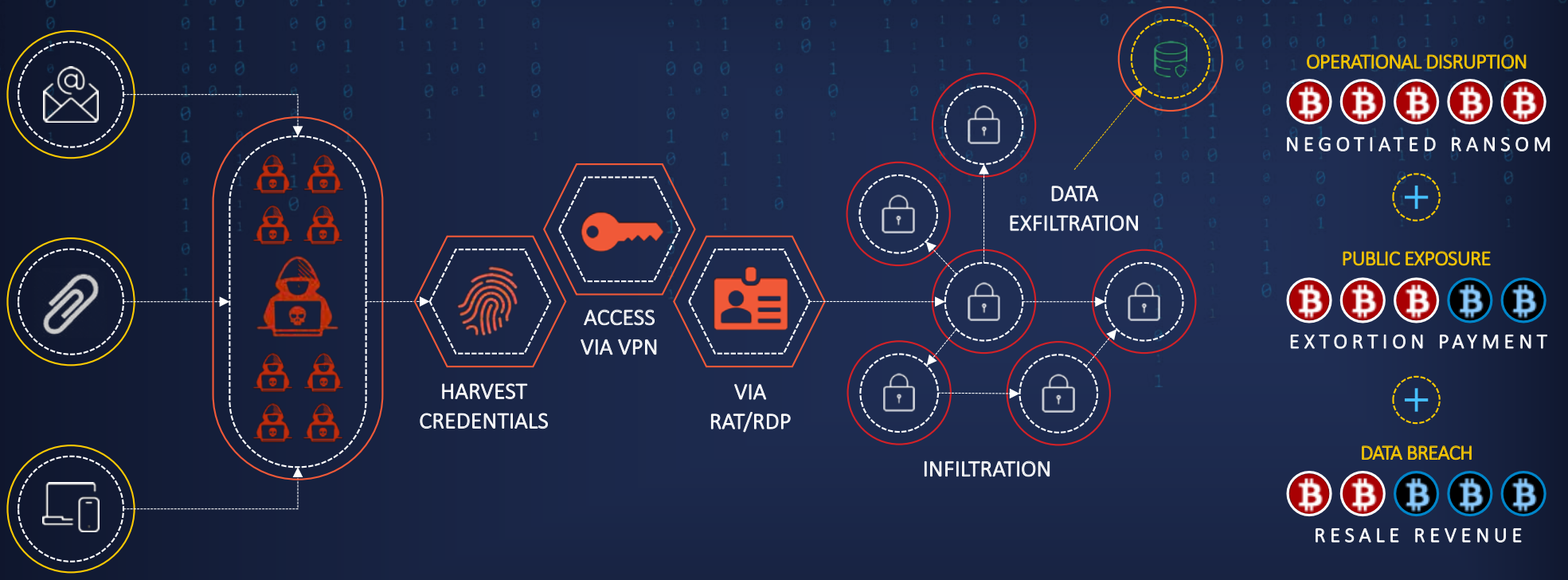
This is how you *think* phishing works

Self-evidently fake emails leading to transactional ransoms

eSENTIRE

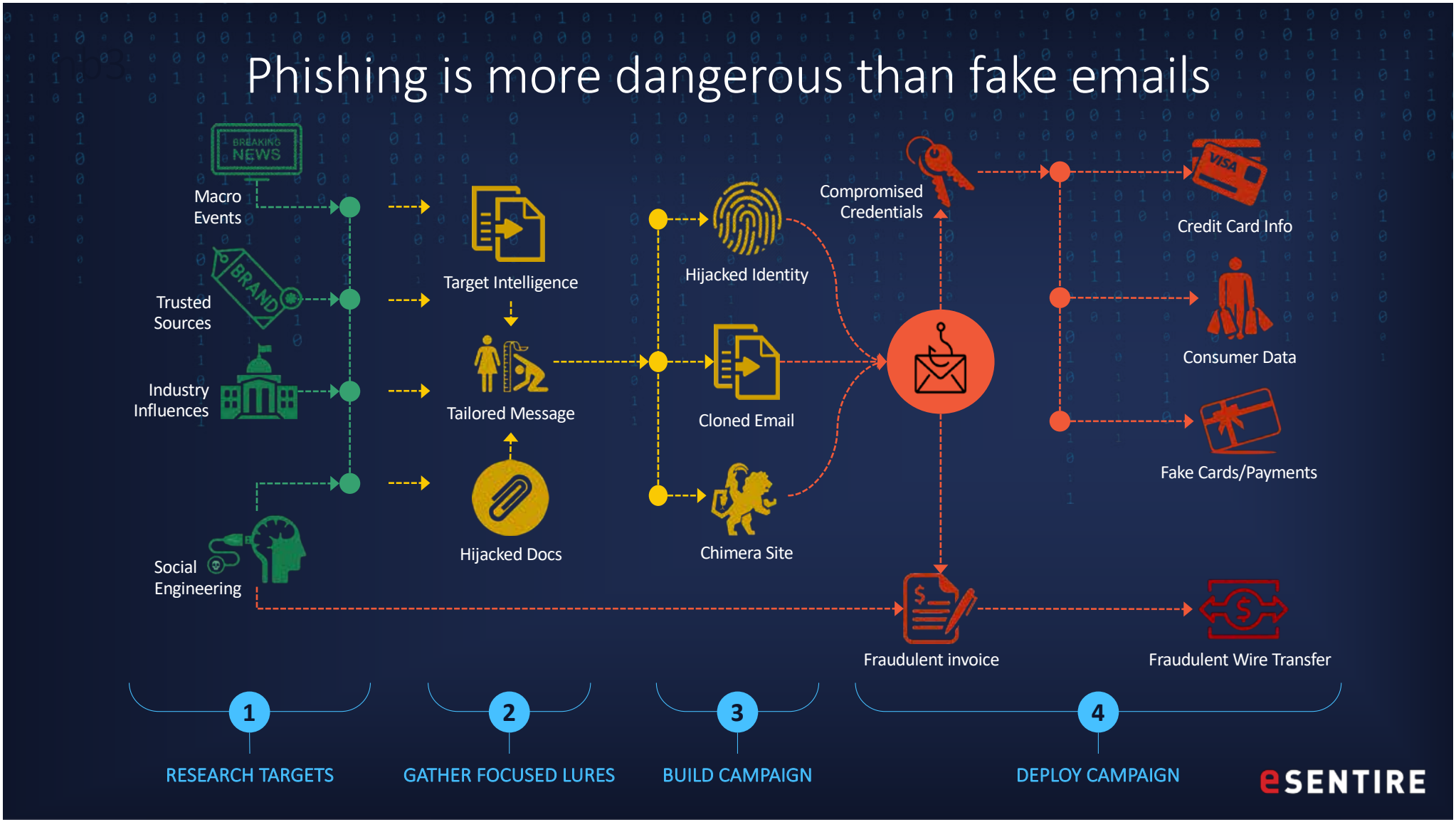
This is how phishing and cyber campaigns *actually* work

Complex and persistent campaigns to create a major security event and six-figure ransoms



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.

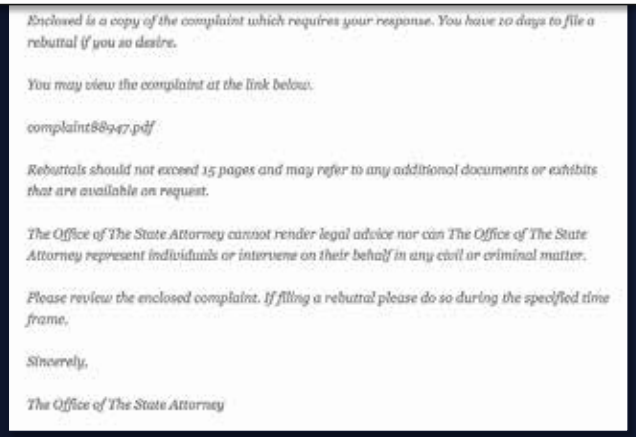
http://share.iu.s3.amazonaws.com/Interview_Assignment.doc

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 can set aside some time to go over it. This next week though, time is very limited. The week after is open. Let me know!



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

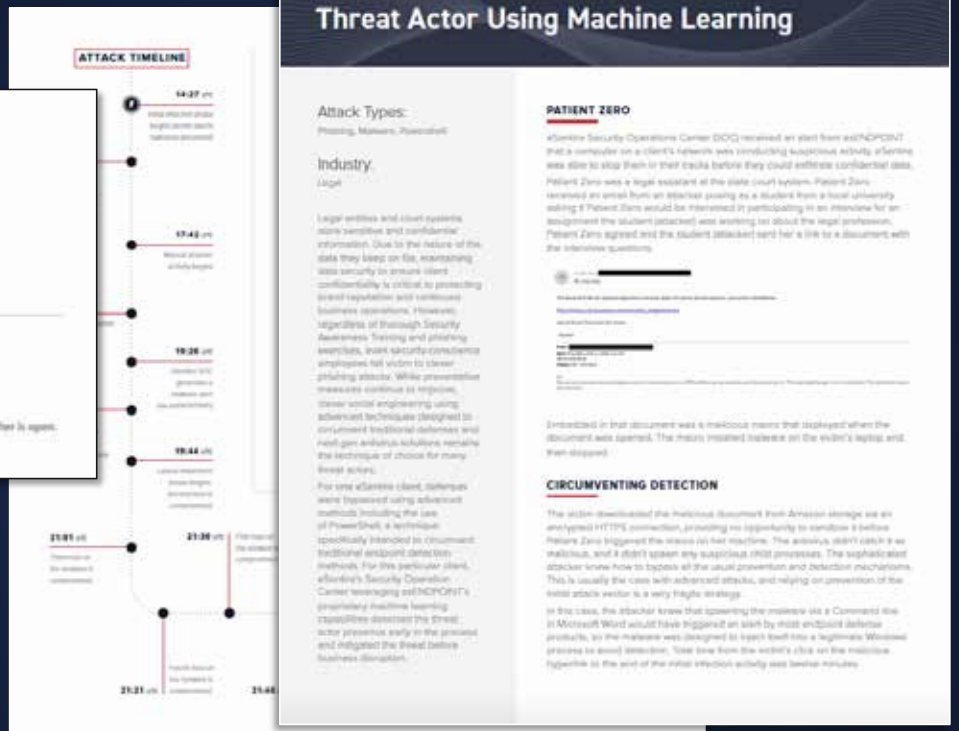
Rebuttals should not exceed 15 pages and may refer to any additional documents or exhibits that are available on request.

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



eSENTIRE

CASE STUDY

esENDPOINT Thwarts Advanced Threat Actor Using Machine Learning

Attack Types:

Phishing, Malware, Powershell

Industry

Legal

Legal entities and court systems store sensitive and confidential information. Due to the nature of the data they keep on file, maintaining data security to ensure client confidentiality is critical to protecting brand reputation and continued business operations. However, regardless of thorough Security Awareness Training and phishing exercises, even security-conscious employees fall victim to clever phishing attacks. While preventative measures continue to improve, clever social engineering using advanced techniques designed to circumvent traditional defenses and next-gen antivirus solutions remains the technique of choice for many threat actors.

For one eSentire client, defenses were bypassed using advanced methods including the use of PowerShell, a technique specifically intended to circumvent traditional endpoint detection methods. For this particular client, eSentire's Security Operation Center leveraging esENDPOINT's proprietary machine learning capabilities detected the threat actor presence early in the process and mitigated the threat before business disruption.

PATIENT ZERO

eSentire Security Operations Center (SOC) received an alert from esENDPOINT that a computer on a client's network was conducting suspicious activity. eSentire was able to stop them in their tracks before they could exfiltrate confidential data.

Patient Zero was a legal assistant at the state court system. Patient Zero received an email from an attacker posing as a student from a local university asking if Patient Zero would be interested in participating in an interview for an assignment the student (attacker) was working on about the legal profession. Patient Zero agreed and the student (attacker) sent her a link to a document with the interview questions.

[redacted]

Embedded in that document was a malicious macro that deployed when the document was opened. The macro installed malware on the victim's laptop and then stopped.

CIRCUMVENTING DETECTION

The victim downloaded the malicious document from Amazon storage via an encrypted HTTPS connection, providing no opportunity to sandbox it before Patient Zero triggered the macro on her machine. The antivirus didn't catch it as malicious, and it didn't spawn any suspicious child processes. The sophisticated attacker knew how to bypass all the usual prevention and detection mechanisms. This is usually the case with advanced attacks, and relying on prevention of the initial attack vector is a very fragile strategy.

In this case, the attacker knew that spawning the malware via a Command line in Microsoft Word would have triggered an alert by most endpoint defense products, so the malware was designed to inject itself into a legitimate Windows process to avoid detection. Total time from the victim's click on the malicious hyperlink to the end of the initial infection activity was twelve minutes.

eSENTIRE

eSENTIRE

BGH: Big Game Hunting

Customized tools and services to identify and exploit target firms

CrowdStrike Intelligence attributed the operation of Ryuk ransomware to WIZARD SPIDER, the well-established criminal adversary behind the TrickBot banking trojan. WIZARD SPIDER continues to develop TrickBot, offering customized modules with government or business themes to identify victims of interest, steal SMS messages containing two-factor authentication (2FA) tokens, and other exploitation tools.

USD ($M)	Bitcoin	Malware
27.7	3,530	Ryuk
18.5	2,349	REvil
18.5	1,278	Maze
18.2	1,440	DopplePalmer
1.6	216	BitPalmer

CrowdStrike: Ransomware developers sell access to distributors (customers) through a partnership program. The program is operated under a financial model that splits profit per infection between the developers and distributors.

eSENTIRE

The industrialization of cybercrime

Best-in-class expertise and as-a-service tools and trade

Ransomware-as-a-Service (RaaS): $140M Business

Because ransomware-as-a-service lowers the entry barriers for prospective cybercrime entrepreneurs, it has the very real potential to increase the "supply" of ransomware operators. Naturally, such an increase will create a larger number of threats for legitimate organizations.

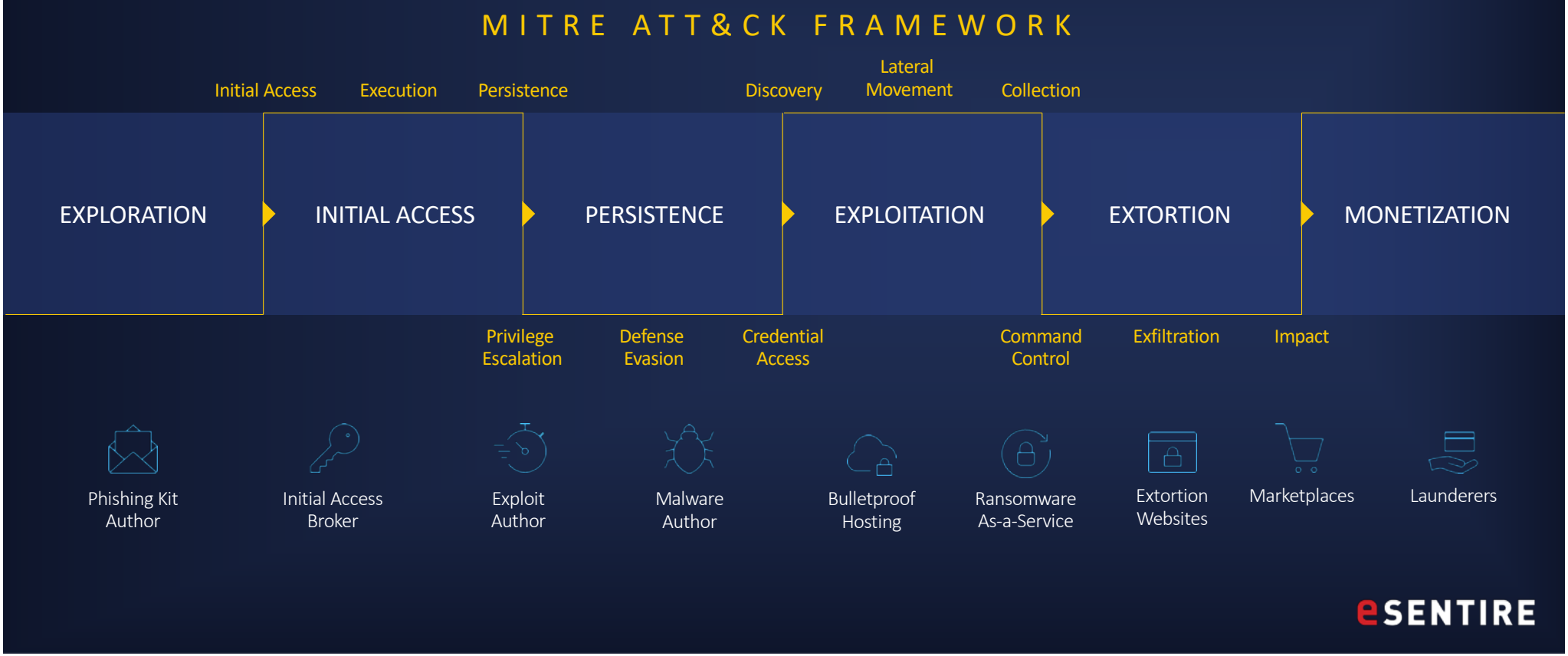
Vmware Carbon Black: Custom malware is now being used in 50 percent of the attacks reported by respondents demonstrating the scale of the dark web, where such malware and malware services can be purchased to empower traditional criminals, spies and terrorists, many of whom do not have the sophisticated resources to execute these attacks.

CrowdStrike: PINCHY SPIDER pioneered the RaaS model of operations, in which the developer receives a share of the profits that affiliates collect from successful ransomware infections. Beginning in February 2019, this adversary advertised its intention to partner with individuals skilled in RDP/VNC networks and with spammers who have experience in corporate networking.

eSENTIRE

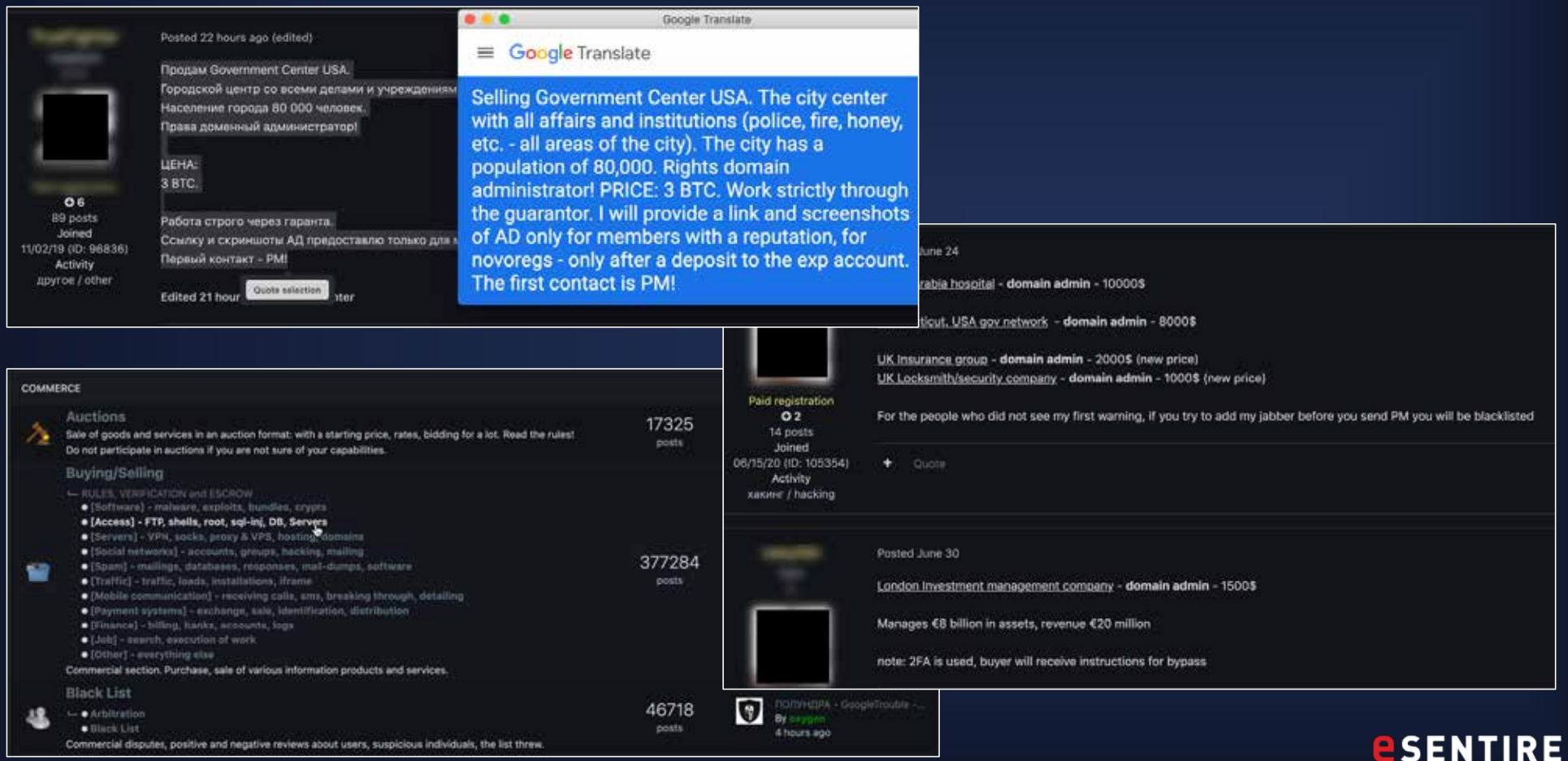
The industrialization of cybercrime

Customized tools and services to identify and exploit target firms



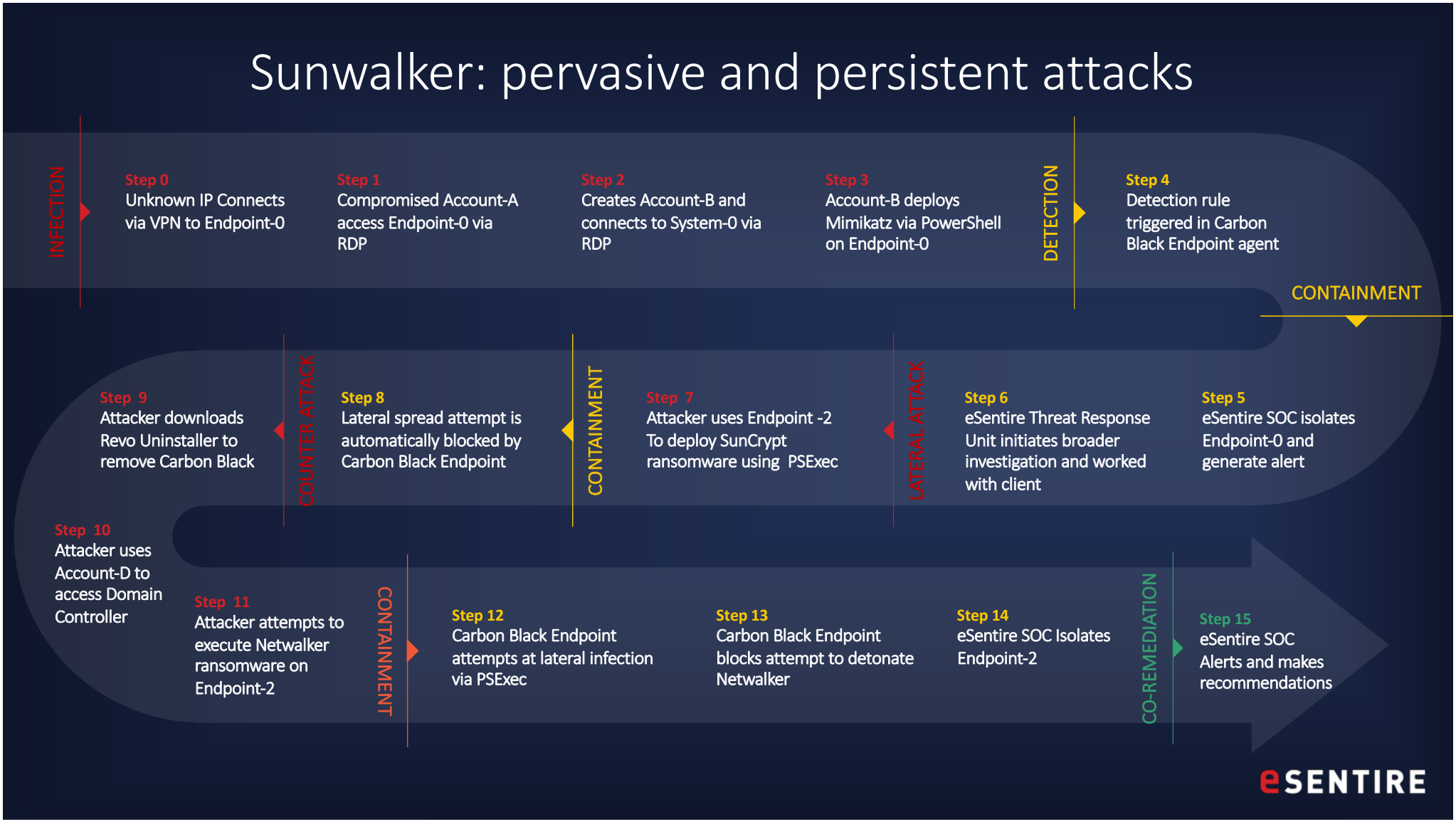
eSENTIRE

Example criminal marketplaces



eSENTIRE

Sunwalker: pervasive and persistent attacks



Standing your ground against cyberattacks

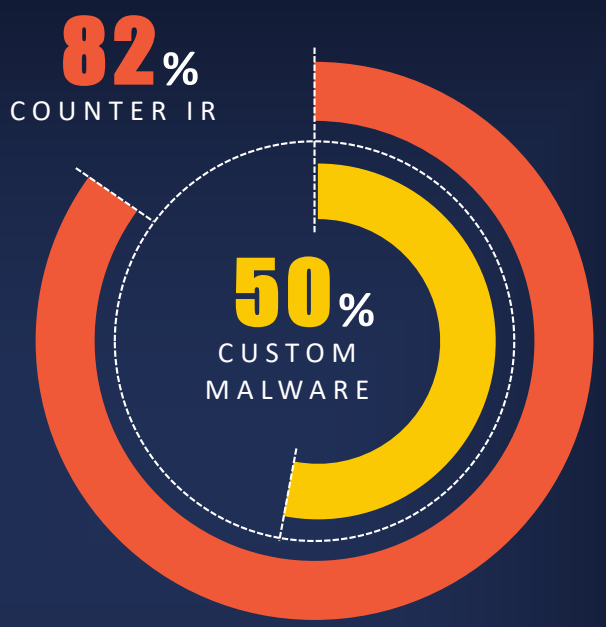
When you turn the lights on an adversary, assume an escalation

1. **ESTABLISH SECURE COMMUNICATIONS**
   Out-of-band communications to coordinate your response following your IR plan

2. **ASSUME MULTIPLE INTRUSIONS**
   Adversaries will "island hop" when one intrusion avenue is detected and contained

3. **NEVER ASSUME A CYBER SINGULARITY**
   Build a program to detect and respond to protracted events. Never assume a singularity

4. **AIRGAP PERSONAL AND BUSINESS**
   Segment personal and business systems, and assume attackers can island hop



eSENTIRE

We all play a role in protecting the firm

Cybersecurity is not an IT problem to solve—it's a business risk to manage

1 Understand the CYBER RISKS

- Read your cybersecurity bulletins
- Do not use personal email/shares for business transactions
- Do not share credentials
- Avoid clicking links (log in instead)
- Follow security/finance controls
- Report suspicious activity

2 Secure your HOME OFFICE

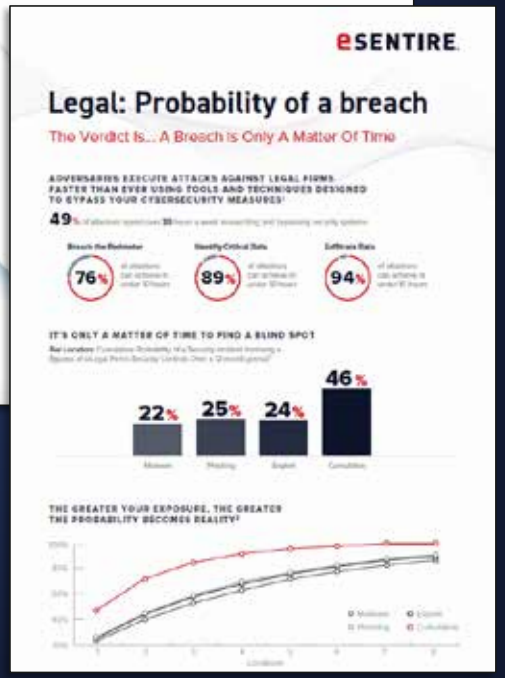
- Keep your kids off your business devices
- Keep your devices up to date
- Censure your social media posts
- Securely manage sensitive data
- Protect virtual meetings
- Consider what's on display during virtual meetings

3 Secure your HOME NETWORK

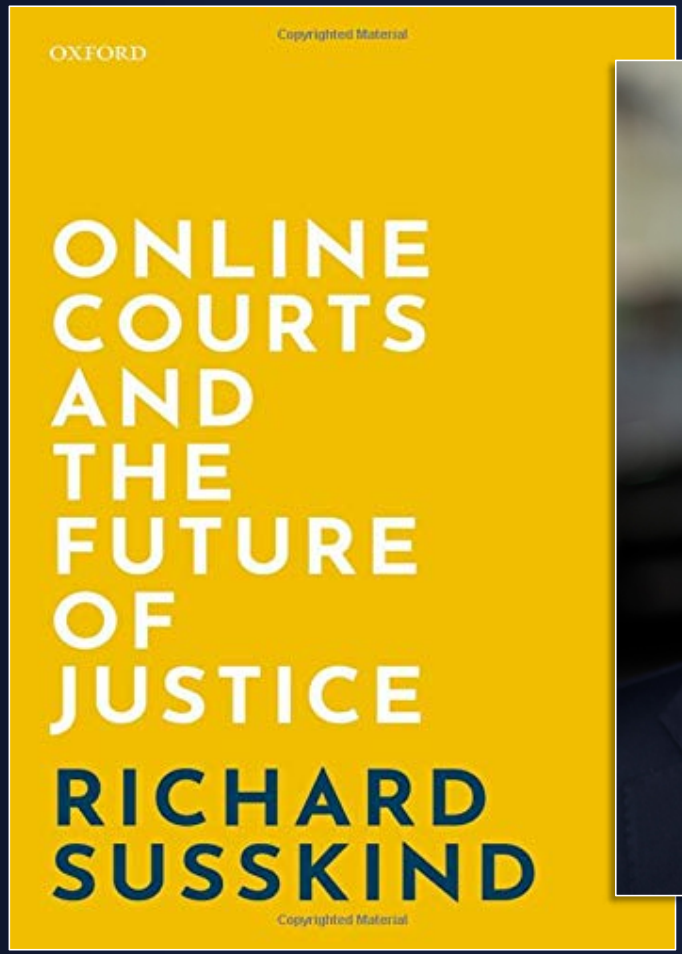
- Change the default Admin credentials on your ISP router
- Change the default name of your WIFI network (SSID)
- Enable WIFI encryption (WPA2 or WPA2 AES)
- Set a strong password need to join your WIFI network
- Create a guest account to share with non-family members
- Always keep your ISP router software up to date

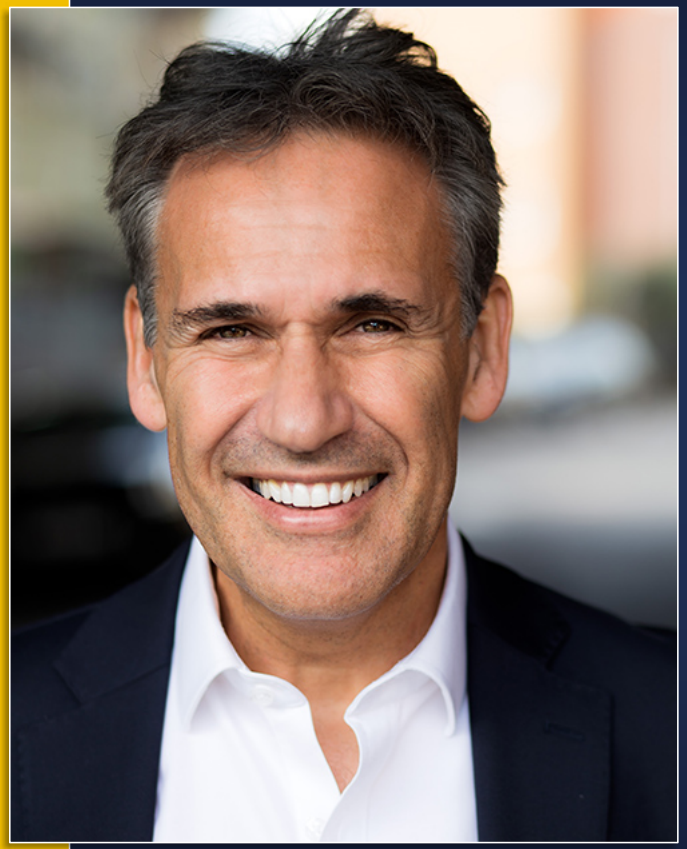
eSENTIRE

Public references



eSENTIRE





Professor Richard Susskind OBE

Professor Richard Susskind OBE is an author, speaker, and independent adviser to major professional firms and to national governments. His main area of expertise is the future of professional service and, in particular, the way in which the IT and the Internet are changing the work of lawyers. He has worked on legal technology for over 30 years. He lectures internationally, has written many books, and advised on numerous government inquiries.

Richard lectures internationally and has been invited to speak in over 40 countries and has addressed audiences (in person and electronically), numbering more than 250,000. He has written and edited numerous books, including Expert Systems in Law (OUP, 1987), The Future of Law (OUP, 1996), Transforming the Law (OUP, 2000), The Susskind Interviews: Legal Experts in Changing Times (Sweet & Maxwell, 2005), The End of Lawyers? Rethinking the Nature of Legal Services (OUP, 2008), Tomorrow's Lawyers (2013), and has written around 150 columns for The Times. His work has been translated into 10 languages.

eSENTIRE

Mark Sangster

Principal Evangelist and VP
Industry Security Strategies

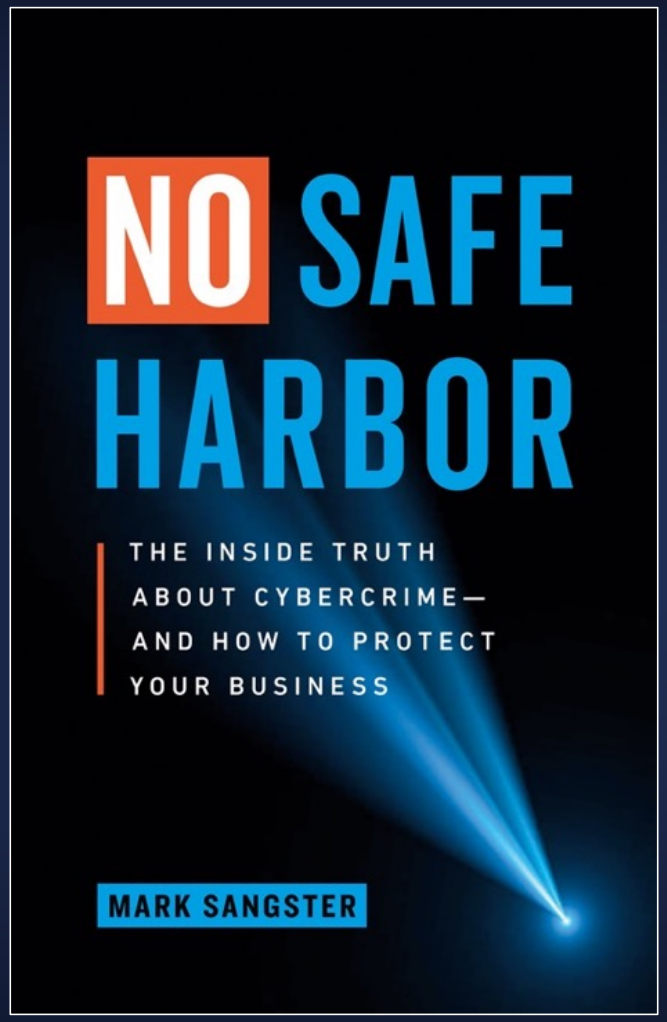
mark.sangster@esentire.com

@mbsangster

Linkedin.com/in/mbsangster

@cyber_mbsangster

mbsangster.com/book



I can't think of anyone better qualified to tell cybersecurity war stories than Mark. This book is a riveting read, filled with details that people don't normally get to hear about.

Danny Bradbury,
Dark Reading

Mark's book gets to the root causes of why there is no safe harbor for any of us. Each chapter lists practical cyber security steps we should all take – starting today!

Mike StJohn-Green,
Independent Cybersecurity Consultant

Mark's advice could not have arrived at a more propitious moment. The book reads like a collection of short stories, all revolving around a central theme: Cybersecurity is a business risk. This book should be essential reading for senior management and corporate directors.

Kenneth Rashbaum,
Partner, Barton LLP

eSENTIRE