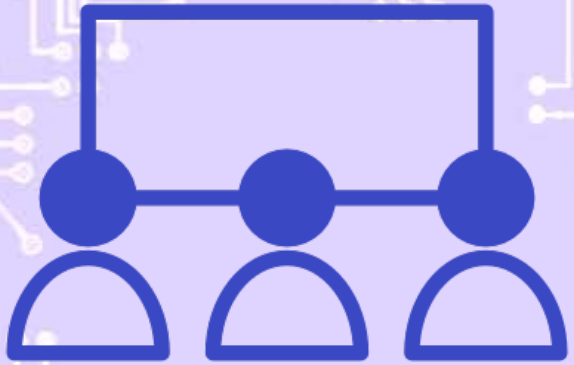
An Ethical Cybersecurity Playbook for Your Law Firm

Abingdon Regional Bench Bar Conference **September 23, 2022**

Sharon Nelson, Esq. & John W. Simek
President and Vice President, Sensei Enterprises, Inc.
snelson@senseient.com; jsimek@senseient.com
senseient.com 703.359.0700

SENSEI'S SERVICES

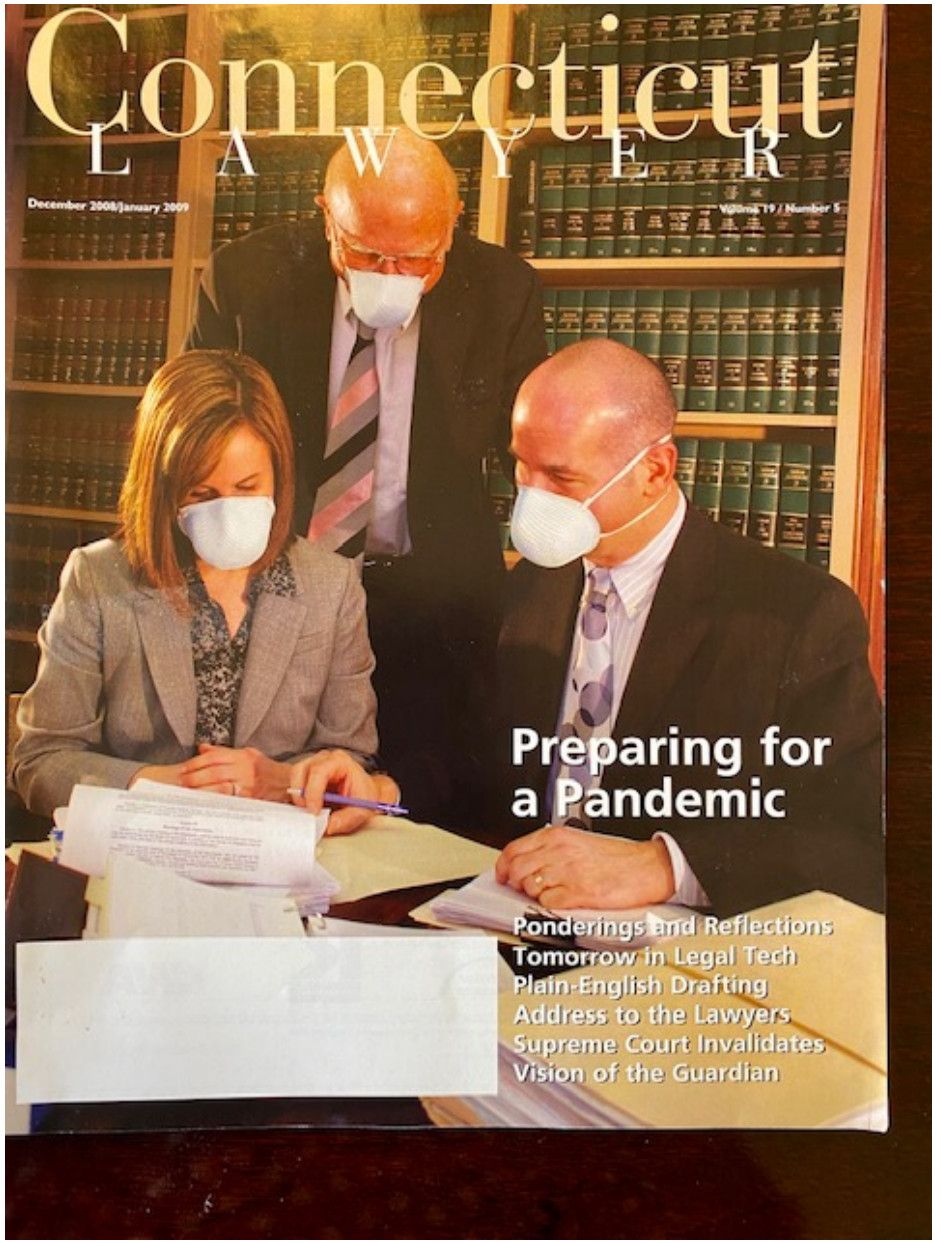
Managed
Information Technology



Managed
Cybersecurity

Digital Forensics

January 2009



Law firms struggle with what “the new normal” looks like

- Work from home 100%
- Fully open at office
- The rise of the hybrid law firm

Work from home? Office? **Hybrid** of both?

- April 2021 survey by global staffing firm Robert Half
- One third of employees who worked at home during the pandemic would look for a new job if required to be in the office fulltime
- 26% want to be fully remote
- 25% want to be fully in the office
- 49% want a hybrid model

How do you protect a hybrid law firm?

- No matter how you operate, it will never be like 2019 again
- Hybrid firms predicted to dominate but as of September 2022, more firms are compelling lawyers to come back to the office, at least several days a week
- Some ethics rules take on new meaning

Ethics
(the big five)

- Rule 1.1 Competence
- Rule 1.4 Communications
- Rule 1.6 Confidentiality
- Rule 5.1 Responsibilities of a Partner or Supervisory Lawyer
- Rule 5.3 Responsibilities Regarding Non-Lawyer Assistance

Competent and Reasonable Measures

01

Know it.

02

Learn it.

03

Get qualified help.

Qualified Consultant

Managed Service Provider (MSP)

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

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 in 2012, address the risks that accompany the benefits of the use of technology by lawyers. When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.

Introduction[1]

Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers.[2] In one highly publicized incident, hackers infiltrated the computer networks at some of the country's most well-known law firms, likely looking for confidential information to exploit through insider trading schemes.[3] Indeed, the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be.[4]

In Formal Opinion 477R, this Committee explained a lawyer's ethical responsibility to use reasonable efforts when communicating client confidential information using the Internet.[5] This

---

[1] This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2018. The laws, court rules, regulations, rules of professional conduct and opinions promulgated in individual jurisdictions are controlling.

[2] *See, e.g.*, Dan Steiner, *Hackers Are Aggressively Targeting Law Firms' Data* (Aug. 3, 2017), https://www.cio.com (explaining that "[f]rom patent disputes to employment contracts, law firms have a lot of exposure to sensitive information. Because of their involvement, confidential information is stored on the enterprise systems that law firms use. . . . This makes them a juicy target for hackers that want to steal consumer information and corporate intelligence."); *See also Criminal-Seeking-Hacker' Requests Network Breach for Insider Trading*, Private Industry Notification 160304-01, FBI, CYBER DIVISION (Mar. 4, 2016).

[3] Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL ST. J. (Mar. 29, 2016), https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504.

[4] Robert S. Mueller, III, *Combatting Threats in the Cyber World Outsmarting Terrorists, Hackers and Spies*, FBI (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[5] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) ("Securing Communication of Protected Client Information").

The elephant in the room

- Cybersecurity - we have lost control of data security
- Federal involvement and a possible federal data breach law to replace the patchwork of state laws
- Data privacy regulation – GDPR, California, Colorado, Virginia (1/1/2023), Utah (12/31/2023) - and a possible federal law

Breached law firms in the headlines

25% of Law Firms Have Been Breached

- ABA's 2021 Legal Technology Survey Report
- Summary by David G. Ries
- https://www.americanbar.org/groups/law_practice/publications/techreport/2021/cybersecurity/

Whether or not you make the headlines, your response is critical – ethically, legally and from a PR standpoint

To avoid the headless chicken response, you need a playbook

ABA Formal Opinion 483: Lawyers' Obligations After an Electronic Data Breach or Cyberattack – 10/17/18

- For background, see ABA Formal Opinion 477R explaining lawyer's ethical responsibility to use reasonable efforts when communicating confidential client information via the internet.
- Opinion 483 – obligations after a breach and addresses only breaches that involve information relating to client representation.

ABA Formal Opinion 483: Lawyers' Obligations After an Electronic Data Breach or Cyberattack – 10/17/18

- **Does not address other laws re: privacy, data breach notifications, HIPAA, Graham-Leach-Bliley, etc.**
- Compliance with this opinion depends on nature of cyber incident, ability of attorney to know the facts about it, the attorney's roles, level of authority and responsibility in law firm's operation

Cyber incident vs. data breach

- **Cyber incident** - Refers to any occurrence that threatens the confidentiality, integrity or availability of information. This might be the result of a cyber attack, perimeter breach or an insider threat (including policy violations).
- **Data breach** – Unauthorized access to data? Data exfiltrated (taken)? Both? Risk of harm?
- No uniform definitions

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

- Rules 1.1 and 1.6 – Lawyers must use and maintain technology used to represent clients and must use it in a manner that reasonably safeguards information
- Competence obligation met through lawyer's own study or employing/retaining qualified assistance
- Obligation to monitor for a data breach
- Many cyber events are not breaches because client confidential information is not compromised
- What about ransomware? It depends.

Obligation to monitor for a data breach

- Monitor access to data
- Unauthorized access
- Logging
- IDS/IPS
- Typically, breached months before discovery

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

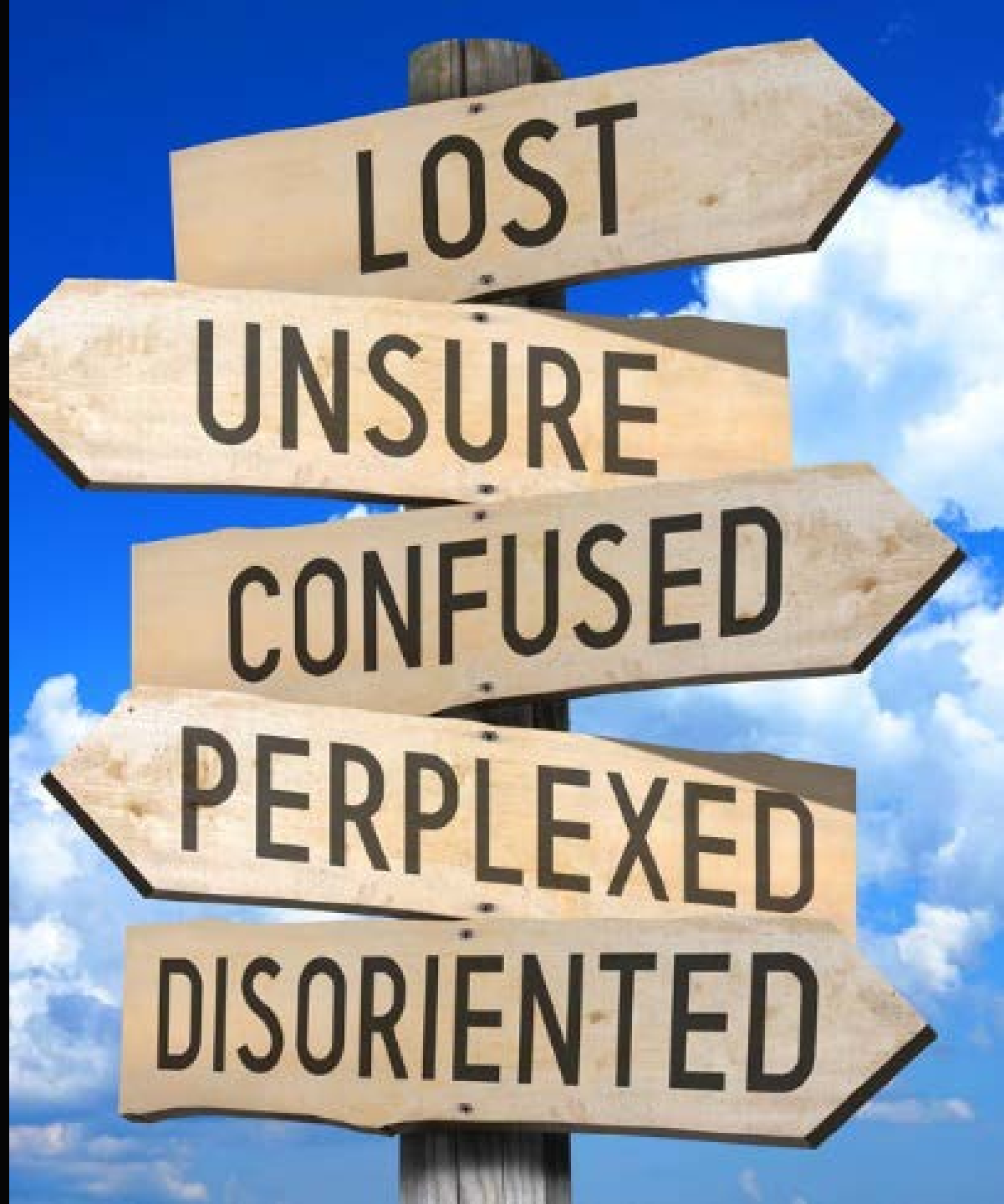
- Lawyers must employ ***reasonable efforts*** to monitor technology, resources connected to the internet, external data sources and external vendors providing data services
- Potential for ethics violation occurs when a lawyer doesn't undertake ***reasonable efforts*** to avoid data loss or to detect cyber-intrusion and that lack of reasonable effort causes the breach

Stopping the Breach and Restoring Systems

- When breach is suspected or detected, Rule 1.1 requires lawyers to act reasonably and promptly to stop the breach and mitigate damage
- How is beyond scope of the opinion
- Lawyers should have an Incident Response Plan – do you have one?
- IRPs minimize loss or theft of information and disruption of services

Why should you have an incident response plan?

- Avoid acting out of panic
- Detect security incidents
- Limit chances of a breach
- Limit financial damages
- Limit data shared and/lost
- Limit the distribution of misinformation
- Limit reputational damage



Everyone has a plan until they get punched in the mouth

Or as the military puts it . . . No plan survives first contact with the enemy

- You can’t afford to be paralyzed
- Especially if a breach or attack is public
- Be ready to think fast and move fast
- Team planning
- Reach out to experts

Why law firms don’t have IRPs

- “We don’t need one – we’re too small to be in danger.”
- “Developing an IRP is expensive and time-consuming.”
- “We have cyberinsurance.”

Cyberinsurance

- Average price hike of 30% - 40% in 2021, sometimes with less coverage!
- Some carriers will no longer cover ransomware payments or nation-state attacks
- Insurance companies may require employee training
- Insurance companies may require security assessments
- Applications are MUCH longer and more complex
- MFA and EDR requirements

Problems with cyberinsurance

- No one knows what the policy language means
- Denial of claims
- The growing number of court cases
- A notification is not a claim

Incident response plan

- Templates are only a start! (Often a bad one)
  - Each entity is different
- Titles of those responsible for plan functions
  - identify a team leader who: understands tech and business; and
  - is a good problem solver/people person
- Critical stakeholders across entity:
  - Management
  - Legal
  - HR
  - IT/IS
  - Communications/PR
  - Compliance

Incident response plan

- Contact info – data breach lawyer #1 call
- Contact info – Organizations should report anomalous cyber activity and/or cyber incidents 24/7 to report@cisa.gov or (888) 282-0870 - will help respond/mitigate
- FBI regional office
  - https://www.fbi.gov/contact-us/field-offices or the Internet Crime Complaint Center (IC3) https://www.ic3.gov/ (faster to respond than FBI)
  - FBI collects info, does not remediate
- Contact info – digital forensics company (investigate, contain, remediate)
- Contact info – insurance policy (attach policy)
- Attach data breach notification law
- Contact info – banks
- Contact info – PR firm

Incident response plan

- Assess data compromised
- PII? PHI? PCI?
- Determine applicable laws:
  - GDPR?
  - HIPAA?
  - GLBA?
  - CCPA?
  - COPPA?
  - Other regulated data?
- Preserve system logs and DLP or IDS data
- Inform employees?
  - When?

Incident response plan

- Informing third parties
  - Vendors
  - Clients
- Train on the plan regularly
  - Tabletop
  - In-person
  - Online
- Add and subtract issues
- Annual review of plan
- After an incident:
  - do a “hot wash” and revise plan as needed

Where to store your Incident Response Plan?

- Ethical duty to be prepared for data breaches
- Firms have been hit with ransomware and unable to access IRP
- Multiple paper copies
- Store on external device not connected to network
- Update the IRP at least annually

Cybersecurity

- **Enemy #1 ransomware**
- Enemy #2 – Business email compromise (BEC) attacks

Forbes

Mar 12, 2021, 08:50am EST | 930 views

Ransomware Attackers Take Aim At Law Firms

AJ Shankar Forbes Councils Member
Forbes Technology Council COUNCIL POST | Membership (fee-based)
Innovation

CEO and Co-Founder at Everlaw — cloud-based software for litigation and investigations.

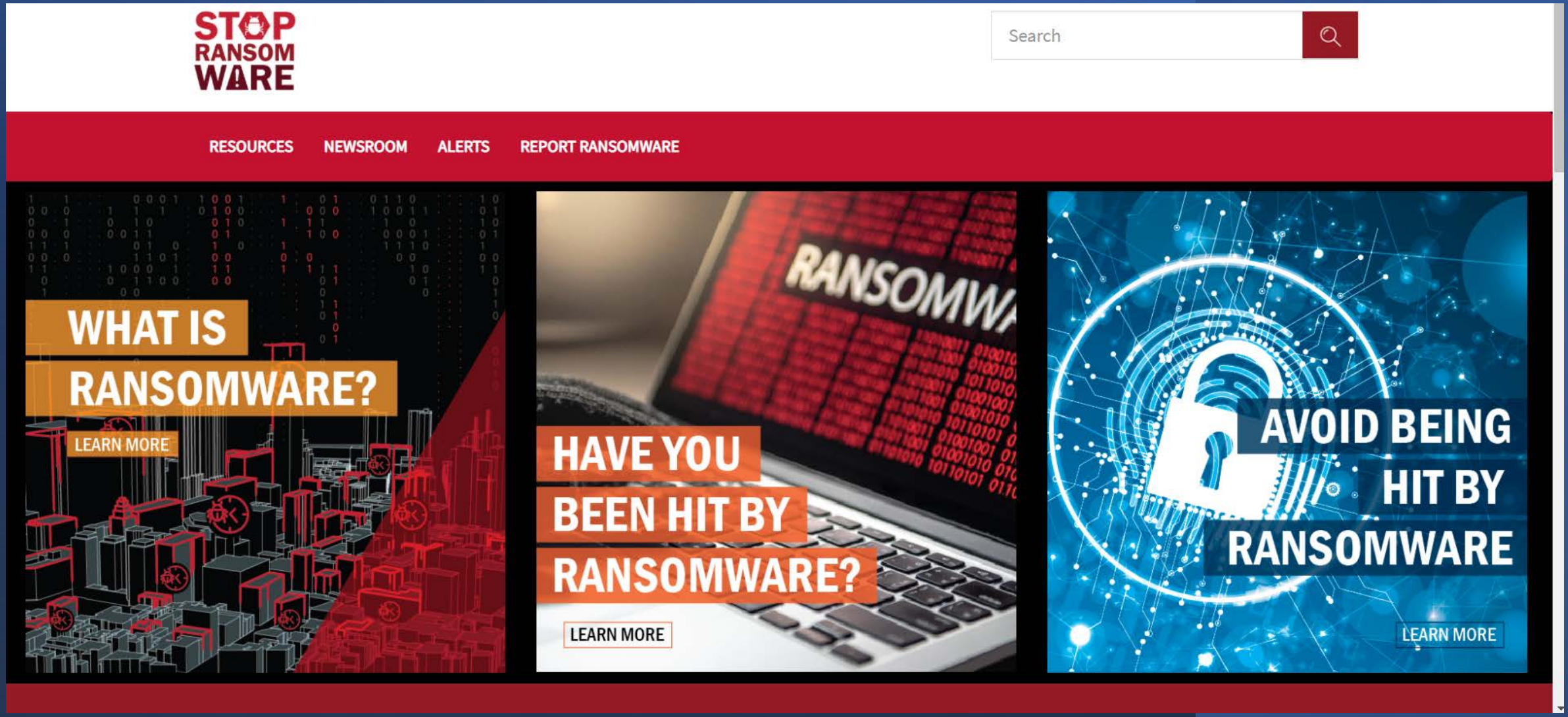
GETTY

March 12, 2021

"…law firms are increasingly an attractive target because of the nature of their business. In the course of corporate legal and M&A work, litigation and other legal services they perform, law firms and in-house legal teams collect tons of confidential corporate information and sensitive data like tax returns. They can suffer reputational and financial losses if they are breached, especially if data is exposed."

A One Stop Shop Resource from CISA

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY



SHIELDS UP

Russia's invasion of Ukraine could impact organizations both within and beyond the region, to include **malicious cyber activity** against the U.S. homeland, including as a response to the unprecedented economic costs imposed on Russia by the U.S. and our allies and partners. Evolving intelligence indicates that the Russian Government is exploring options for potential cyberattacks. Every organization—large and small—must be prepared to respond to disruptive cyber incidents. As the nation's cyber defense agency, CISA stands ready to help organizations prepare for, respond to, and mitigate the impact of cyberattacks. When cyber incidents are reported quickly, we can use this information to render assistance and as warning to prevent other organizations and entities from falling victim to a similar attack.

Organizations should report anomalous cyber activity and/or cyber incidents 24/7 to report@cisa.gov or (888) 282-0870.

Latest Updates

Ransomware 1.0 Definition

- Form of malware
- Designed to encrypt files on a device/network
- Attackers then demand ransom (generally Bitcoin) to get the decryption key

Ransomware 2.0

- Targeted ransomware
- Data exfiltration – a data breach?
- Sell or release data
- Encrypt or destroy backups
- Legal fines (e.g. HIPAA, GDPR, OFAC)
- Financial loss
- Reputational damage
- Bankruptcy

How bad is ransomware? Really, really bad

- Blockchain analytics firm Chainanalysis (reported Feb. 2022)
- Over $692 million paid in 2020, more than four times what was paid in 2019
- $602 million paid in 2021
- 2021 – over 140 ransomware strains
- 2021 – average payment $118K+
- Ransomware negotiation is a new cottage industry
- Ransomware now comprises 75% of cyberinsurance claims (AM Best)

Assumptions from Coveware - 2021

- Data will not be credibly destroyed, but traded to others, sold, misplaced or held for a second extortion attempt
- Exfiltrated data was held by multiple parties and not secured. Any of them may have made copies for future extortion
- Data may be deliberately or mistakenly published before victim can respond

Coveware stats re: law firms - 2021

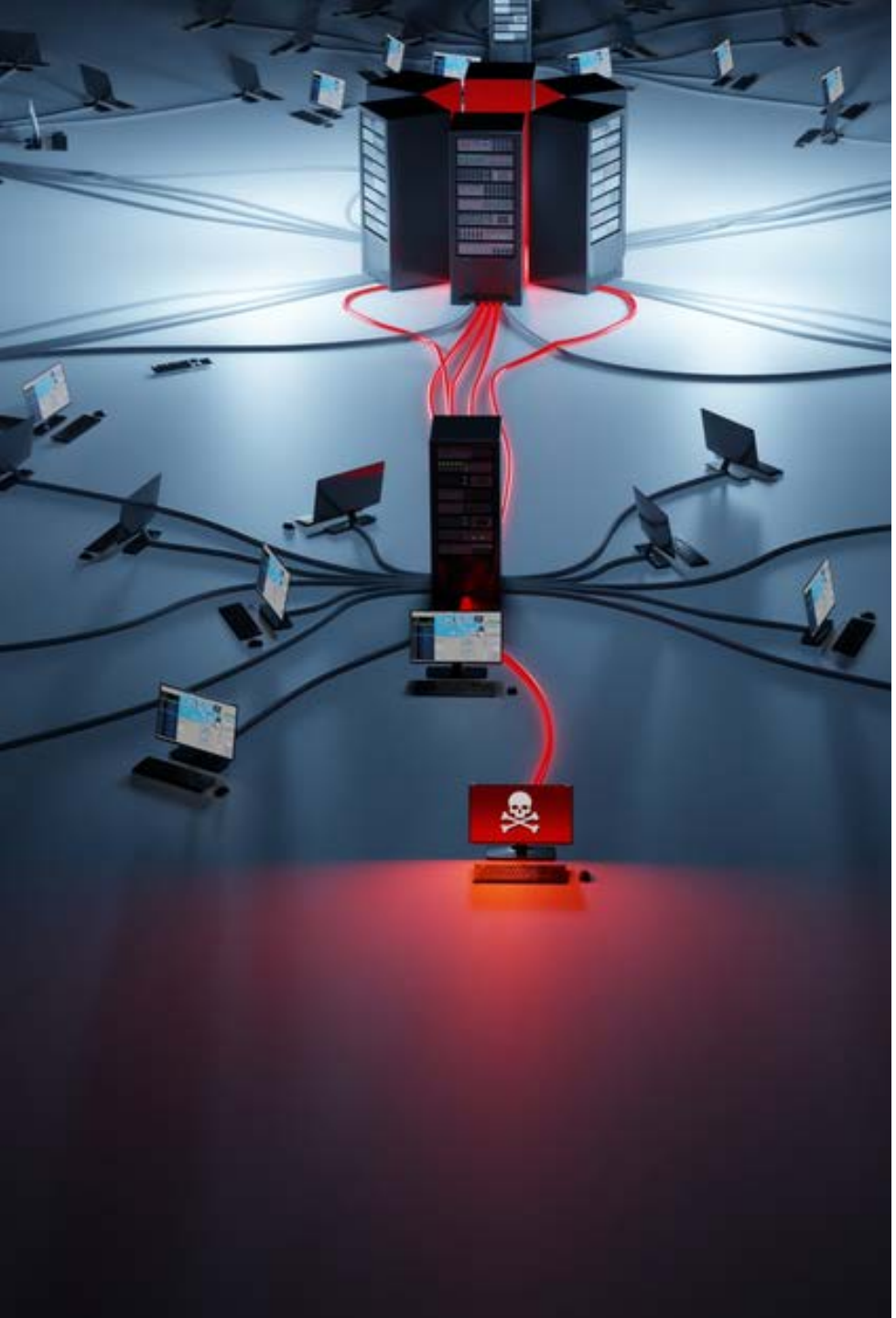
- 24.9% of attacks target professional services firms, especially small and midsize law firms
- Budget hobbles them
- So does desire to maximize profits and income to the partners
- Clients are smaller and may not demand security assessments
- Attacks don’t often make headlines
- Don’t properly handle attacks or remediation

Sophos: The State of Ransomware in 2021

- Only 8% of entities get back ALL their data after paying ransom
- 29% get back no more than half their data
- Remediation costs 10X size of ransom payment on average

Most common ransomware attack vectors

1. Compromised remote desktop protocol (RDP)
2. Phishing emails
3. Software vulnerabilities



Ransomware defenses

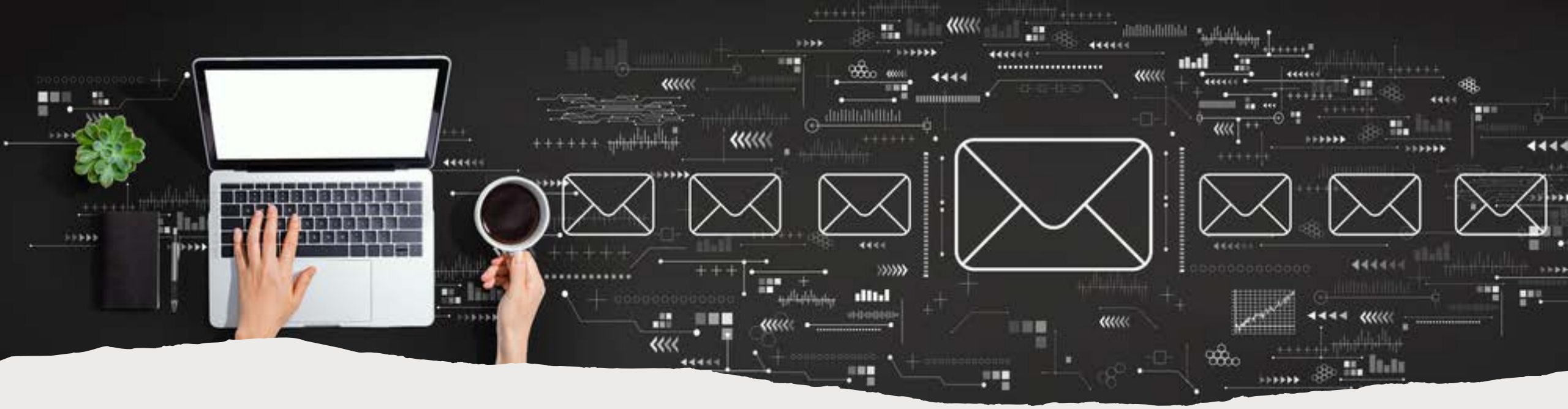
- Maintain, test, and secure backups so they can't be deleted or encrypted.
- Control or disable network services. Stop using Remote Desktop Protocol!
- Least privilege access.

Patches and updates

- Attackers move right after a vulnerability is discovered knowing that many people don’t patch right away
- Operating system and third-party updates
- Prompt patching reduces vulnerabilities
- Often can be scheduled and automated (with a trusted 3rd party testing the patch before installing)
- “We have a no patch policy. Patches break things.”

Cybersecurity awareness training

- Once or twice a year
- Repetitive training required
- Make training mandatory



Endpoint protection and email filtering

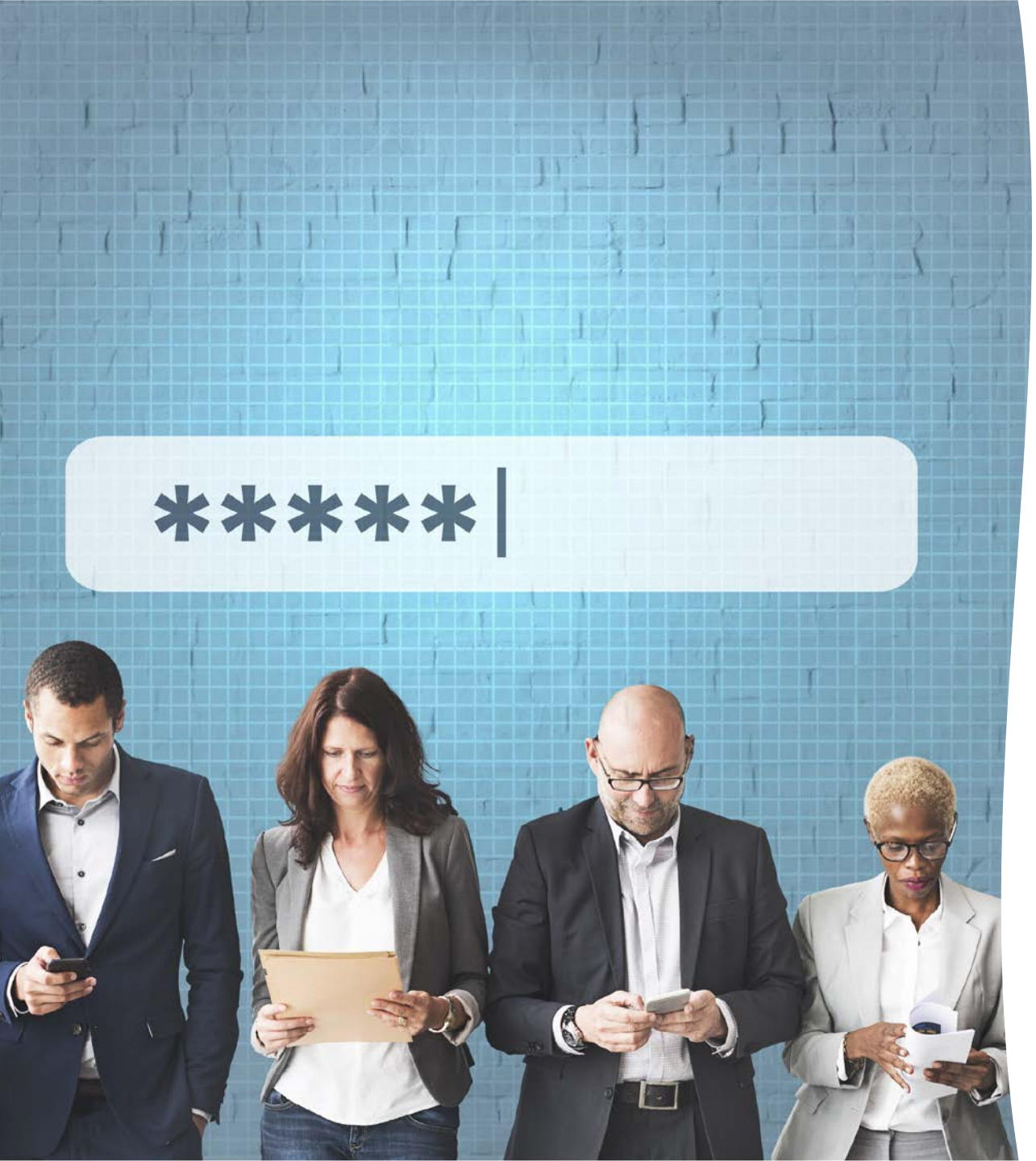
- May be a solution combination, e.g. Webroot SecureAnywhere and SentinelOne
- Advance threat protection, ransomware detection and response
- Heuristic learning
- Artificial intelligence and machine learning
- Scheduled scans/actively monitoring users and system processes
- Some can roll back to a “known good state” and work with a SOC (Security Operations Center) to analyze dangerous activities

Cybersecurity (MFA)

- Multifactor authentication (MFA) – included free with Microsoft 365 but must be configured
- Microsoft study showed that MFA stops 99.9% of credential-based compromises (Account Takeover attacks)

The most secure way to use 2FA?

- #4 Have code texted to phone, (can be intercepted using SIM swapping or tricking you into entering the code on a false logon screen) LEAST SECURE (but way better than nothing!)
- #3 Use an authentication app (generates a new code every 30 seconds)
- #2 Use push notifications, which you can simply accept
- #1 Use a hardware token MOST SECURE



Deploy a strong password policy

- Make sure the strong password policy is enforced – no password reuse or sharing passwords!
- 50% do share passwords, 1/3 write passwords down, 83% have access to accounts from past employers!!!!
- Passwords should be 14 characters or more – numbers, lower and upper case, special characters – withstand brute force attacks

VPN Alert!

- VPN attacks up nearly 2000% in the hybrid workplace (Nuspire June 2021)
- VPNs have vulnerabilities. Make sure the latest Windows/macOS security updates and patches are installed
- MUST use MFA (multifactor authentication) with your VPN and other remote access solutions

Business email compromise attacks (BEC)

- Spoofs a trusted individual (CEO/CFO)
- Convinces recipient to send financial info
- Purchase gift cards
- Fraudulent wire transfers – e.g. change invoice data to redirect payments to a known vendor
- Utilizing virtual meeting platforms.
- Immediately transferred to cryptocurrency wallets and dispersed
- IC3 2021 Internet Crime Report – BEC $2.4 billion

The “New Normal” will include “**Zero Trust**”

- Zero Trust no longer assumes that actors, systems or services operating from within the security perimeter should be automatically trusted, and instead we must verify anything and everything trying to connect to its systems before granting access
- Perimeter security model no longer works
- Even the perimeter itself no longer clearly defined – why?

The “New Normal” will include “**Zero Trust**”

- Applications and data are stored on-premise and in the cloud with users accessing them from multiple devices and locations
- Gartner: By 2022 80% of business applications with be accessed by zero trust network access (ZTNA) and by 2023 60% of business will phase out remote access virtual networks (VPNs) in favor of ZTNA.

SENSEI ENTERPRISES

DIGITAL FORENSICS | INFORMATION TECHNOLOGY | CYBERSECURITY

ANY QUESTIONS?

Sharon Nelson, Esq. and John W. Simek

President and Vice President of Sensei Enterprises, Inc.

snelson@senseient.com; jsimek@senseient.com

senseient.com 703.359.0700