asae foresightWORKS

Fraying Cybersecurity

SUMMARY: Risks to digital infrastructures are growing, even as dependence on them rises and more of everyday life is conducted via a digital layer. The workforce is both worried and harried—concerned about digital privacy and security in the workplace, and tired of the difficulty and complexity of maintaining system security. Associations face the same risks as other organizations but also have opportunities to support members in new ways.

Forecasts

- Risks to cybersecurity will continue to grow in both numbers and potential for harm, driven by the rise in cyberwarfare activities by governments, expansion of the internet of things (IoT), and the growing sophistication of the global criminal marketplace for stolen data.
- The IoT will create billions of new vectors of attack, from infrastructure systems and toys to medical devices and door locks. The Economist Intelligence Unit has called the IoT "a quantum leap in cyber-risk."
- Cybersecurity will increasingly be unmanageable by humans. An emerging genre of AI will automate cyber-defense, automatically detecting and self-healing systemic risks.
- In the wake of public infrastructure ransom and malware attacks, governments are likely to pay more attention to public cybersecurity—potentially even treating it as a "public health" issue, with new regulations for consumer-facing companies and IoT products.
- The increasing digitalization of personal services—banking, cryptocurrency, electronic health records, personal fitness data—will also increase personal vulnerability to cyber-attacks.

Key Uncertainties

The scale and scope of future digital disasters

•

Risks from the internet of things and how effectively they are addressed

•

Whether courts will extend existing liability protections for non-internet products (e.g., cars, appliances) to the IoT

•

Whether autonomous cybersecurity systems will be as effective as hoped

•

Shifts in balance between cyber offense and defense

Supporting Trends

- **Cybersecurity insurance.** The cybersecurity insurance market is growing slowly despite increasing cyber-attacks. It's currently small, with only $5 billion in premiums.
- **Cybercrime-as-a-service.** A growing suite of tools, from exploit kits to ransomware, are available to help cybercriminals build threats and launch attacks.
- **Concern about online privacy.** Americans are very worried about the privacy of their personal data online.
- **Online-security fatigue.** Consumers are feeling "security fatigue" from the growing security concerns about their personal and professional information.
- **Internet of things.** The internet of things is spreading rapidly.
- **Wearable technologies.** Wearables will continue to grow and expand further into domains like payment and health monitoring.
- **The fragmenting internet.** The internet is de-globalizing as governments seek to have more control over its content and uses.
- **Counter-surveillance apps.** As revelations about government intrusion into private communications create new concerns about electronic privacy, new mobile apps and other secure-communications software are gaining popularity.
- **5G and cybersecurity.** Security experts identified four aspects of 5G that increase risks: more extensive or dangerous attacks due to a larger pool of connected devices; more insecure IoT devices on network; increased network data traffic making it harder to see or track threats; and inherent insecurity of 5G network devices due to vulnerable engineering.
- ~~**Wariness of Chinese tech.** China's push for dominance in next-gen technologies,~~

Related Drivers of Change

- The Surveillance Economy
- Personalized Artificial Intelligence
- Fast Data
- Algorithms and Rights

Notable Data Points

ATTACKS ON CRITICAL INFRASTRUCTURE

Baltimore spent $6 million
to secure and harden its systems after a ransomware attack.
Atlanta spent $2.6 million to recover from a similar attack.

Source: Ellen Cranley, "8 Cities That Have Been Crippled By Cyberattacks—And What They Did To Fight Them," Business Insider, January 27, 2020.

THE COSTS OF CYBERCRIME

According to the FBI,
cybercrime cost Americans $6.9 billion
in damages in 2021.

Source: Chris Brook, "Cybercrime Cost U.S. $6.9 billion in 2021," Data Insider, March 23, 2022.

CRYPTOCURRENCY THEFT

In 2021,
thieves and scammers stole $14 billion in cryptocurrency,
an estimated 516% over 2020 figures.

Sources: MacKenzie Sigalos, Crypto Scammers Took a Record $14 Billion in 2021, CNBC.com, January 6, 2022.

Strategic Insights

- Both for themselves and for members, associations will need to understand the shifting responsibilities of organizations:
  - How should companies protect their employees?
  - How can associations best protect sensitive member data?
  - Are organizations responsible when an employee is maliciously trolled or doxed via their systems?
- Industries will need to respond to the vulnerabilities created by the growth of the internet of things. Associations can educate their members about risks and opportunities and the best tools for managing each.
- Cyberattacks can include corporate espionage. Associations may be subject to attacks and should keep their staff updated in threat identification.
- Cybersecurity insurance, a small but growing market, can protect against catastrophic financial and/or reputation loss from data breaches. Besides buying it themselves, some associations might find it useful to offer cybersecurity insurance as a member benefit, in partnership with an insurance firm.
- Humans are a weak link in organizations' cybersecurity regimes. Associations can serve as educators and advocates of employee-related best practices.
- Increased regulatory attention to cybersecurity could open a window for associations to help shape the regulatory environment to benefit members.

Timing

- **Stage:** Growth, both in terms of risks and threats proliferating, and of new security solutions reaching market-readiness
- **Speed:** Rapid in terms of both threats and potential remedies

Potential Alternative Futures

- **Radical transparency:** With massive amounts of data about everyone readily available, identity theft is obsolete because a system can tell if users are who they claim to be.
- **The internet as walled gardens:** No longer a vast, open playground, the internet is a maze of walled gardens secluded behind firewalls and paid memberships.
- **Don't touch my data:** Effective, secure online frameworks emerge to help ordinary people take control of their data and manage who can see it and use it.

Take Action

- **Get cybersecurity out of IT and onto the board agenda.** Cybersecurity is a substantive and serious issue for all associations and businesses. Boards have a fiduciary responsibility to act to secure the association and a leadership responsibility to help members respond to this challenge. Do the risk analysis and invest in mitigation.
- **Have a business continuity plan.** Assume you will be hit directly or taken offline by cyberattack at some point. Plan how you will redirect business and communication systems to alternative platforms to avoid disruption.
- **Educate aggressively on the changing nature of industry threats.** Offer prompt and continuous updates via alerts, webinars, and technical reports to give members the tools to defend their organizations. Assemble and share best practices. Train staff how to be vigilant and work with IT on a strong line of defense.
- **Protect member data from intrusion.** Build safeguards around data to ensure privacy and protect members against identity theft.
- **Explore new services and partnerships that make strong security affordable.** Small businesses and local affiliates may not be able to afford higher levels of security expertise and systems. Consider how you might broker technical expertise and support as a new member service. Investigate the potential to create a "walled garden" where members can interact with additional measures of security not found elsewhere.

Keyword Search

To continue researching this change driver, use combinations of these search terms: *risk, security, cybersecurity, hacking, cybercrime, cyberwarfare, cyberattack, cyberdefense, privacy, internet of things, IoT, surveillance, data breach, trolling, dox, doxing, data ownership, malware, spyware, bot net, ransomware*

Who Will Be Affected

All businesses and organizations are vulnerable to cybersecurity breaches. Mission-critical industries like healthcare, utilities, and transportation need solutions to contribute to national security. Retail and finance industries handle high volumes of sensitive data. Associations will need technology partners to respond.

About ASAE ForesightWorks

ASAE ForesightWorks is a deliberate, evidence-based research program and emerging line of products to provide association professionals with a continual stream of intelligence about the changes facing the association industry, including:

- regularly updated action briefs;
- tools for applying insights from the research in your association;
- guidance in performing environmental scans; and
- opportunities to engage with peers around the research.

Ultimately, the program's mission is to empower association leaders to create a culture of foresight.

Check **asaecenter.org/ForesightWorks** and follow **@ASAEfdn** on Twitter for updates on new findings and events.

SUPPORTING TRENDS

such as AI and mobile networks, along with a growing view of China as a security and economic threat, are driving wariness toward the country's tech exports and companies.