IDEAS
ACTION
RESULTS

Top Risks in Cybersecurity 2023

February 2023

Bipartisan Policy Center

CONTRIBUTORS

Tom Romanoff
Director of the Technology Project for the Bipartisan Policy Center

Sabine Neschke
Policy Analyst, Technology Project, Bipartisan Policy Center

Danielle Draper
Project Coordinator, Technology Project, Bipartisan Policy Center

Jamil Farshchi
EVP and Chief Information Security Officer, Equifax

Ben Lord
Executive Communications Specialist, Security, Equifax

Ahmad Douglas
Chief Security Officer, Equifax Workforce Solutions

WORKING GROUP CHAIRS

Jamil Farshchi
EVP and Chief Information Security Officer of Equifax

Tom Romanoff
Director of the Technology Project for the Bipartisan Policy Center

WORKING GROUP MEMBERS

Christopher Painter
Former Cybersecurity Leader at the U.S. Department of State, Department of Justice, and the White House

Craig Froelich
Chief Information Security Officer of Bank of America

Hon. Jim Langevin
Member of the U.S. House of Representatives and Chair of the Subcommittee on Cyber, Innovative Technologies, and Information Systems

Hon. Mark Brnovich
Attorney General of the State of Arizona

Hon. Sean Reyes
Attorney General of the State of Utah

Jeremy Grant
Coordinator of the Better Identity Coalition and former Senior Executive Advisor for NIST

Jerry Davis
Founder Gryphon X

Jules Polonetsky
CEO of the Future of Privacy Forum

Noopur Davis
EVP and Chief Information Security and Product Privacy Officer of Comcast

Phil Venables
Chief Information Security Officer of Google Cloud

RADM (Ret.) Mark Montgomery
Executive Director of Cyberspace Solarium Commission 2.0.

ACKNOWLEDGMENTS

BPC thanks Equifax for its generous support and partnership for this project. The authors are grateful to all the participants from industry, government, and civil society who partook in the working group, including Jason Isaak and Evan Burke, and offered their feedback as part of the report writing process.

DISCLAIMER

Table of Contents

Introduction to BPC and the Report

BPC AND THE WORKING GROUP

The Bipartisan Policy Center (BPC) convened a working group of leaders to strengthen America's cybersecurity. The group's approach was to identify the nation's top cybersecurity risks to raise awareness so policymakers and businesses can take pragmatic action and invest in countermeasures.

In assembling the working group, the co-chairs sought broad inclusivity from strategically important industries, government, and civil society. Every sector with a stake in cybersecurity was included – banking, communications, digital platforms, health, energy, and more. The working group drew from a wide range of important perspectives, including stakeholders representing privacy concerns and digital identities.

IN THE REPORT

Identifying cybersecurity risks is the first step in managing them. This report – unlike other, more technical sources that identify cyber risks – frames them for the strategic audience of business and government decision-makers. We intentionally focused on identifying risks, not solutions, because various stakeholders may need to take different approaches. There are no one-size-fits-all fixes. Rather, these top risks must be considered individually by companies and collectively by the nation. Many will require a multifaceted response, across business and government, who will need to work various levers including policy, organizational culture, technology, and processes.

OVERVIEW OF THE TOP 2023 CYBERSECURITY RISKS

Top Macro Risks

These top eight macro risks represent a consolidation of the most likely and impactful of the risks identified by the working group. Each risk's description includes "Key Risk Factors," which identify concrete examples or hazards that fall under the identified risk. The listed key factors are starting points – they are not exhaustive.

Other Notable Risks

This section contains the extended list of macro risks and risk factors identified by the working group. These either did not fit into one of the eight top macro risk sections or did not have a specific 2023 focus.

Top Macro Risks

EVOLVING GEOPOLITICAL ENVIRONMENT

The multilateral geopolitical landscape is evolving and has been influenced recently by several factors, including increasing international conflict and a broader trend toward nationalism. Perhaps the most significant emerging factor is the growing number of cyberattacks and attempts to disrupt critical infrastructure resulting from the war between Russia and Ukraine; the war runs the risk of spilling outside the immediate conflict zone. Growing tensions between Western nations and China have aggravated more frequent and impactful malicious cyber activities as countries pursue their national interests. Additionally, conflicts in the Middle East increase the likelihood of cyberattacks in the region, with rivals seeking to promote certain ideologies or discredit adversaries. While these conflicts may be localized, cyber threats can have far-reaching effects given the global nature of the internet. The Internet and other technologies have allowed actors to carry out these activities remotely and nearly instantaneously.

The United States has actively worked to enhance its cybersecurity with its NATO and treaty allies, and to implement effective cybersecurity measures to protect critical infrastructure and government systems. While the U.S. has aggressively pursued policies to address risks, we have identified several risk factors that will require continued attention and increased countermeasures in 2023.

Key Risk Factors

- ***Lowered inhibitions for cyberattacks***
  Perceived anonymity, slow and imprecise attribution, and the remote nature of the attacks make cyberattacks attractive to nation-states. Espionage, sabotage, and "false flag" attacks are all appealing – with inhibitions lower, and the likelihood of success higher, than at any time in recent memory.

Some governments incentivize nonstate cybercriminals to work as proxies, expanding their cyber talent base.

- ***State-sponsored physical and cyberattacks on critical infrastructure***
  Attacks on undersea cables and basic infrastructure, such as utilities and logistics, can have enormous repercussions for a region or even the entire world. These types of attacks increased in 2022 and remain a top risk going into 2023.[1]
- ***Mis- and disinformation campaigns***
  Social media and other technologies can be used for good but also for mischief. Adversarial nation-states, groups organized around fringe beliefs, or lone-wolf individuals controlling "bots" can influence the general public's opinion in an effort to undermine elections, public health initiatives, or public order. With these campaigns increasing in scale, social media and other online platforms are struggling to implement effective, socially, and politically acceptable policies, leading us to anticipate that these campaigns will reach an even broader audience in 2023.
- ***Protectionist approaches to trade***
  Countries have implemented supply chain restrictions and reduced trade in reaction to geopolitical and economic developments, as well as to protect against malicious vendors under nation-state influence. However, protectionism can leave companies that have already purchased products from these vendors even more vulnerable – unable to update their hardware and software. Also, the flow of top talent may be restricted, affecting global innovation.

ACCELERATING CYBER ARMS RACE

The fundamental nature of cybersecurity is ever expanding. Attack methods that are decades old can still work, and with each new innovation from attackers, defenders must figure out how to defend against past, present, and future attacks – without incurring an unsustainable increase in the cost of defense.

Superimposed on this basic, difficult reality is an "arms race" between attackers and beleaguered defenders. Rapid and continual advancements in offensive and defensive capabilities require defenders to keep pace in an environment that disproportionately favors attackers. Advances in artificial intelligence simultaneously offer great opportunity and danger, the democratization of advanced attack techniques, and unprecedented automation/scalability. All considered, the surface area that cybersecurity professionals must protect will grow exponentially throughout 2023 as technology advances and digitization further underpin modern economies, national security, and society.

Key Risk Factors

- ***Criminals leveraging commonly available consumer technology for illicit purposes***
  Bad actors often co-opt commonly available technologies in new ways for use in criminal activity. Technologies such as social media, encryption, and AI-generated content have become indispensable tools for cybercriminals and escalated their ability to reach victims. Governments and the companies that operate online platforms often struggle to implement effective, transparent, credible, and legally defensible safeguards.
- ***Attacking the human factor of strong controls***
  No matter how advanced the control is, human factors usually provide an avenue to bypass it. For example, hackers have recently devised ways to circumvent multifactor authentication (MFA), a historically strong control, by tricking individuals into approving illegitimate access requests. Blocking these exploitations often generates friction, as users are forced to expend extra time and effort to access an online account. Ultimately, this leads to a trade-off of risk mitigation at the expense of productivity and vice versa, which may harm the business's perception of the security function and strain important cross-functional partnerships.
- ***Threats to national security***
  The U.S. Department of Defense and other federal agencies faced countless cyberattacks in 2022, and this trend is likely to continue in 2023.[2] As federal agencies increasingly partner with private-sector companies in emerging fields such as satellites and telecommunications, the challenges of protecting these cyber-dependent national security assets must remain a key issue for policymakers in 2023.

GLOBAL ECONOMIC HEADWINDS

Stock market volatility and steep inflation have affected global demand and triggered shocks to global supply chains and key elements of the world economy. A 2022 survey of supply chain executives found that 92 percent of respondents had changed their supply chain footprint, and 90 percent of these respondents said they would pursue regionalization during the next three years, underscoring that fundamental changes to the global economy will continue.[3] The expectation for continued market volatility and higher interest rates in 2023 exacerbates the unstable geopolitical environment and poses risks across the cybersecurity sector.[4]

In economically uncertain times, businesses and governments will need to make difficult decisions about allocating resources, including personnel, budgets, and time. These decisions can create or increase cybersecurity risks – either directly by reducing spending on cybersecurity or indirectly by deferring costly but important updates to their operating environments and

corresponding controls. Cybersecurity is not immune to recessions— research indicates that cyberattacks increase during and following economic downturns, such as the 22.3 percent increase in cybercrime documented by the FBI after the 2008 recession.[5] With a recession potentially on the horizon, the private and public sectors may face heightened cybersecurity risks, while addressing difficult resource allocation decisions.

Key Risk Factors

- ***Challenging revenue and expense environment***
  Businesses might assume more security risks by delaying their mergers and acquisition (M&A) integration, slowing the decommissioning of end-of-life and vulnerable software and hardware, or deferring cyber hygiene activities. Delays could increase organizational risks and slow incorporation of innovative cyber technologies.
- ***Long-term investments limited by short-term cost reductions***
  The cost of labor to operate multiyear and fixed-cost cybersecurity technology investments, as well as a corresponding inability to automate routine cybersecurity tasks, could jeopardize an organization's ability to benefit from their investments and defend against common threats.
- ***Risks to startups could lead to less innovation***
  Startups, which possess less reserve capital and are exposed earlier and more heavily to market downturns than established companies, might suffer if economic headwinds continue into 2023. Because cybersecurity startups serve a critical innovation role in helping to identify and counter emerging cybersecurity threats, organizations may be less able to keep pace with the evolving threat landscape.

OVERLAPPING, CONFLICTING, AND SUBJECTIVE REGULATIONS

In the United States, and internationally as a consequence of their global nexus, companies navigate the complex patchwork of required cybersecurity, data security, and privacy regulations implemented by national, state, and local authorities, with varying prescriptive requirements. Current laws mandate that organizations must report security incidents within a specific time frame, anywhere from hours to days after the occurrence. However, more clarity is needed on how and whether an incident must be confirmed prior to its being reportable. We must consider the challenges these requirements create for global companies navigating a patchwork of regulations governing data sovereignty, localization, and privacy. Failure to engage the business community and various stakeholders to understand their priorities may result in further unintended consequences. Governments, businesses, regulators, and

policymakers will need to grapple with this expanding policy landscape as the number of laws increases and their requirements further diverge.

Key Risk Factors

- ***Balkanization of data privacy and breach disclosure laws***
  As of January 2023, five U.S. states have enacted comprehensive consumer privacy laws, with many other states considering it. At the same time, a number of states have rolled out digital IDs. However, each of these states has its own digital legal apparatus, multiplying the complexity and cost for organizations needing to comply. A disproportionate burden falls on medium-sized businesses that aspire to do business more broadly but lack the legal and compliance sophistication to fully comply with these regulations.
- ***Rapidly elevating cybersecurity control requirements***
  It is common for companies to negotiate specific control requirements with individual business partners as part of the contracting process. Tracking compliance, mapping alignment, and providing meaningful assurance against this increasingly complex compliance landscape is becoming more difficult and expensive for nongovernment organizations.
- ***One-Size-Fits-All regulation***
  In response to more frequent cyber threats, governments are increasing their oversight of the private sector's cybersecurity practices. But cybersecurity is dynamic, tailored uniquely to each organization, and requires a flexible approach. Thus, regulations need to take into account the needs of specific industries and organizations – the various missions they carry out and the types of data they process. As governments and regulators aim to mitigate cyber risks, they might apply a generalized approach that misses key vulnerabilities in some sectors and creates burdensome compliance costs in others.

LAGGING CORPORATE GOVERNANCE

In recent years, the United States has experienced a significant shift toward greater corporate cybersecurity governance, with individuals such as the chief information security officer (CISO) and others with cybersecurity responsibilities becoming more prominent in corporate boardrooms.[6] As these trends continue into 2023, significant vulnerabilities remain to be addressed to ensure cyber readiness in corporate settings. For example, only 45 percent of Fortune 100 companies made a cyber management and oversight disclosure in 2021, and another 46 percent identified cybersecurity as an area of expertise sought on their board.[7] Although large firms have made modest headway adding cyber-savvy talent to corporate boards and senior leadership positions, many firms still lack these positions. They, therefore, have insufficient managerial expertise, accountability, diversity of thought, and oversight to manage their cybersecurity effectively.

Without consistent and standardized corporate governance practices nationally, companies might face an uncertain and challenging operating environment. Small- and medium-sized businesses face an outsized risk from cyber threats, often lacking the infrastructure and expertise to counter cyberattacks adequately.[8] These businesses' vulnerability represents a major risk to the cybersecurity landscape in 2023.

Key Risk Factors

- ***Separating corporate cybersecurity from organizational objectives***
  In some organizations, security is seen as distinct from, or in opposition to, other objectives, effectively absolving the business, information technology, and other functions from taking responsibility for the organization's overall cybersecurity effectiveness. Management can forget that security is an essential *quality* of their mission.
- ***Distance between security professionals and the C-suite***
  Successfully responding to sophisticated cybersecurity threats requires a swift, coordinated response from multiple functions within an organization — up to and including the executive team and board of directors. Although lower-level security staff may have real-time or near real-time access to incident information, the inherent bureaucracy of large organizations inhibits the fast, effective flow of information upward and laterally. Organizations that do not create and maintain a fast path for cybersecurity information and decision making may lose out on opportunities to contain a smaller situation before it becomes a larger one. The absence of a CISO or CSO from the executive ranks may exclude essential context or subject matter expertise from the decision-making path.
- ***Increased oversight through multiple lines of defense***
  If the lines of communication to report cyber threats are not well established or defined, they are not conducive to risk management. Additionally, if the board or management is not informed by other levels within an organization, they may be less able to anticipate emerging threats.
- ***Lack of technical experts on boards of directors***
  Comprehensive cyber governance and oversight are necessary to help identify, address, and mitigate cyber threats. The complexity and sophistication of these threats can make it difficult for overseers without proper domain experience and technical acumen to manage them effectively. Boards without the appropriate expertise may fail to provide direction, exposing the business to threats.

LACK OF INVESTMENT, PREPAREDNESS, AND RESILIENCE

Both the public and private sectors have insufficiently prepared for, or invested in resilience against, a significant cybersecurity disaster, creating a major vulnerability that continues into 2023. Recent victims span industries such as transportation, financial services, streaming media, nonprofit organizations, health care, meatpacking, and energy. On the infrastructure side, ransomware affected more than 200 local governments, schools, and hospitals in the United States in 2022.[9] And these breaches can have life-and-death implications: A survey of victimized health care facilities found a quarter of respondents saw higher mortality rates following a ransomware attack.[10] Overseas, large-scale infrastructure attacks on the U.S. and allies' infrastructure present vulnerabilities and demonstrate the need to be vigilant.

Complacency toward crisis preparedness could also lead to financial consequences or loss of confidential information. Failure to prepare and invest in up-to-date technology can lead to data breaches, phishing attacks, insider threats, and other risks. Reliance on third- and fourth-party operators might also pose additional risks to cyber systems. Even when adequate defense measures are in place, a lack of credible testing or operational resiliency can leave organizations unprepared for emerging threats.

Key Risk Factors

- ***Suboptimal risk decisioning due to incomplete and imperfect data***
  Across the cybersecurity ecosystem, defenders are relying on incomplete and imperfect data. Decision-makers lack comprehensive, timely data and trends on threats, attackers, exploits, and vulnerabilities. The effects are profound: Policymakers cannot offer data-driven recommendations, and organizations cannot effectively prioritize their countermeasures and control investments. Until the cybersecurity data gap is addressed, the inherent asymmetry in cybersecurity that advantages bad actors over defenders will continue.
- ***Lack of crisis preparedness, disaster recovery (DR), and business continuity (BC) planning***
  Formal crisis planning, business continuity, and disaster recovery are essential when dealing with the threat of a cyberattack. However, static plans are insufficient and do not age well. Without periodic resiliency reviews and effective testing of procedures, threats will have greater consequences. Because many of these systems are interconnected, a lack of resilience in one company adds a collective risk to a sector.
- ***Failing to conduct crisis exercises and planning***
  Sterile "tabletop" exercises where participants discuss their role in a hypothetical emergency fail to represent real-life crises. Frequently, such exercises are limited to IT personnel and lower levels of staff. When organizations fail to conduct exercises at all levels, from the board to the subject-matter experts, and do not draw broadly on participants from multiple organizational disciplines, they leave gaps in their crisis response execution.

- ***Vendor risk concentration and insufficient third-party assurance capabilities***
  Overreliance on one firm or one cyber defense strategy can open systems to attacks and other vulnerabilities. But even when the public and private sector diversify their use of cybersecurity products, supply chain security risk management remains immature. Governments and companies overwhelmingly rely on questionnaires and other means that lack verifiable assurance and ongoing recency. Although commercial services are beginning to fill the gap with assessments based on threat intelligence, perimeter scanning, and other measures, a recent study found that only 34 percent of IT security professionals have confidence that a primary third party would notify their partners of a data breach.[11] Meanwhile, in a similar study, a large portion of U.S.-based respondents had experienced significant disruptions due to third parties' cloud breaches (45 percent) or data exfiltration (39 percent).[12]
- ***Escalating cost of cyber insurance***
  The rising costs of cyber insurance might prevent small- and medium-sized businesses (SMBs) from obtaining coverage. SMBs not only rely on cyber insurance to transfer risks but also to receive coaching on breaches and support in the event of an incident. If insurance becomes cost prohibitive, SMBs might find themselves ill-equipped to handle cyberattacks. In addition, some insurers use exclusionary clauses that can give a false impression that a company is covered for incidents.
- ***Poor cyber hygiene and security awareness among the general public***
  Individual negligence significantly contributes to data breaches. A 2022 study found that 82 percent of breaches involved the human element and that phishing was the primary social engineering tactic used.[13] The risk level remains high, as this percentage shows no signs of subsiding. Bad security habits include weak passwords, accidentally clicking on phishing links, losing devices, and inadequate employer-led training.

VULNERABLE INFRASTRUCTURE

Critical infrastructure face unique cybersecurity threats in the United States, as these services have shared public and private responsibilities. The Cybersecurity Information Security Agency (CISA) defines critical infrastructure as the "assets, systems, facilities, networks, and other elements that society relies upon to maintain national security, economic vitality, and public health and safety."[14] Many of these systems rely heavily on state and local agencies and third- and fourth-party vendors who may lack necessary cybersecurity controls. The vulnerability of these relatively smaller operators creates outsize risk due to the broad systemic dependency on their services.

Key Risk Factors

- ***Stability and security of financial infrastructure***
  The financial system is an inherently attractive target for cybercriminals seeking monetary gain. Furthermore, financial interference is a logical strategy for nation-states looking to disrupt entire economies or make a statement against capitalism. Meanwhile, consumers' growing appetite for convenience and choice drives rapid change, including

the convergence of banks and technology companies and steep increases in online banking. This pace of transformation in a historically stable industry might result in gaps in security controls and presents more surface area for hackers to probe for vulnerabilities.

- ***Reliable and safe operation of utilities***
  Electric grids, water plants, other utilities, and basic services underpinning the U.S. economy are all experiencing heightened cyberattacks, threatening the continuity of daily activities. Information technology (IT) and operational technology (OT) pose different risks to digital and physical infrastructure, respectively. Authorities who administer these services may not yet have the appropriate leadership and resources to effectively assess and mitigate the vulnerabilities stemming from the convergence of IT and OT systems.[15]
- ***Trustworthy operation of essential government services***
  Effective and efficient provisioning of services is a basic duty of government at every level – local/municipal, state, and federal. This duty extends beyond election security to essential services such as policing and criminal justice, emergency response, administering social welfare and benefits programs, and attending to medical and food safety. Cyberattacks on government services of all levels will continue and increase in 2023 as part of a broader agenda by malicious actors to delegitimize Western governments and democracy.
- ***Unpatched outdated code and legacy systems***
  Vulnerable software, operating systems, or other infrastructure almost always factor into consequential security incidents and data breaches. Keeping pace with patching and replacing end-of-life software and hardware is a major operational burden for organizations of all sizes. When this need is ignored, the cost, complexity, and likelihood of incidents multiply over time.

TALENT SCARCITY

Organizations struggle to retain cybersecurity personnel, exposing them to cyber risks. The "Great Resignation," remote work, cloud adoption, artificial intelligence, consumer inflationary pressures, and other factors are exacerbating the situation. Only one percent of Fortune 100 companies said they had sufficient in-house digital talent in a 2022 survey, down from 10 percent in 2020.[16] The influence of COVID-driven educational attainment gaps that have yet to manifest might further contribute to the cybersecurity talent shortage. Today's security operations centers are constantly having to hire skilled staff to defend against cloud storage and intelligence-driven attacks and other emerging threats. Without skilled talent to meet these new challenges, organizations' security posture will decline.

Key Risk Factors

- ***Systemic scarcity of trained cybersecurity professionals***
  According to a 2022 Cybersecurity Workforce Study, the United States alone has approximately 700,000 unfilled cybersecurity jobs. That number is set to increase as the demand for trained cybersecurity professionals grows.[17] Wages for skilled practitioners continue to rise due to this demand, coupled with the scarcity in supply, effectively pricing out many government entities and SMBs. Organizations face trade-offs in cybersecurity risk and leaving these roles unfilled.
- ***Insufficient support or automation to meet modernization efforts demand***
  As businesses and government agencies rely more on digital assets to fulfill their core mission, the technology and operational estate under their purview continues to grow. This requires top talent to lead cyber modernization efforts and the labor necessary to execute cybersecurity. Automation can alleviate some of the labor demand but requires further institutional support. If both the automation and labor support are lacking, the most talented cyber professionals will find it impossible to execute and mature cyber operations. The government shares responsibility if the private sector is under-resourced and under-staffed.

Other Notable Risks

Throughout the working group meetings, members identified several risks and threats that merit inclusion in the report, separate from the collective consensus of the top risks. These risks were primarily collected during our brainstorming phase. Their inclusion is meant to provide further insights into the cyber risk/threat landscape and represent opinions from the diverse backgrounds from our working group members. The risks are categorized into two types: strategic risks and operational threats.

Strategic-Level Risks- Represent identified risks that are at the macro-level of cybersecurity concerns. There were no specific threats associated with them, but they could multiply over time. Some were identified as highly probable but not specific to a 2023 timeline.

Operational Threats- Represent micro-level threats to cybersecurity operations. Like the strategic risks identified in this section, some were recognized as probable but not specific to a 2023 timeline. These threats also come from direct experience from the working group and have increased in frequency.

STRATEGIC-LEVEL RISKS

Third-Party Protection of Personally Identifiable Information

Third-party protection of personally identifiable information (PII) refers to the measures taken by organizations to protect the personal data of individuals that they collect, store, or process on behalf of another organization or individual. PII refers to any information that can be used to identify an individual, such as their name, address, phone number, email address, or Social Security number. Organizations often share this information with third parties, such as service providers or partners, for various purposes, such as to perform analytics. Measures to protect the privacy and security of individuals include implementing security controls and protocols, conducting regular security assessments, and complying with relevant laws and regulations. All U.S. states and territories have data breach laws that require companies to inform consumers when a breach has occurred within 10 to 45 days of the breach, depending on the state. Current federal privacy legislation only concerns data in specific contexts and industries.

Lack of a Single Defined Standard of Care

In the cybersecurity context, a standard of care is defined as reasonable and prudent cybersecurity practices. There is no recognized standard of care because of the wide range of organizations' security needs across industries and the economy. The definition can include such things as installing and regularly updating software and security systems, training employees on security best practices, and implementing policies and procedures to prevent unauthorized access to sensitive information. Without a standard in place, different expectations could lead to gaps in cyber coverage. Absent a national standard and action by Congress, California, Indiana, Ohio, and other states have passed cybersecurity laws to address what they consider an appropriate standard of care.[18]

Increased Scale and Severity of Breaches

As the number of global internet users increases annually, the proliferation and reliance on technology enables more cyberattacks than ever before. Cybercrime statistics and trends demonstrate that the number of cyberattacks increases 15 percent every year.[19] Furthermore, remote work presents unique security challenges, and data breaches can compromise home networks and personal devices. As the global threat grows and becomes more sophisticated, nearly every industry has had to implement new strategies and adapt, quickly. Yet, bad actors constantly evolve their methods in response to new countermeasures. Large-scale, complex hacks are expensive, with the average cost of a data breach in the United States at $9.44 million in 2021.[20]

Transparency of Security to Investors

In 2022, the Securities and Exchange Commission proposed new cybersecurity risk management rules requiring investment advisers and public companies to disclose cyber incidents. The working group supports these actions. We believe more clarity is needed about the threshold that makes an incident reportable, and about when the reporting clock starts since there is a gap between the time an incident occurs, the time it is discovered, and the time that it reaches a threshold that makes it reportable. As companies adopt these disclosure requirements, the risk of noncompliance emerges from ill-defined requirements. This challenge combined with the increased transparency and a lack of cyber expertise in the general public could create a false narrative around companies' ability to protect its assets. Policymakers and the public should know that the reception of cyber disclosures through transparency rules will affect companies' stock valuation.

White-Collar Cybercrime

White-collar cybercrime refers to nonviolent, illegal activities that are committed online for financial gain. Examples of these computer crimes include intellectual property theft, computer hacking, credit card fraud,

identity theft, phishing schemes and many more. Likewise, the e-commerce marketplace saw an unprecedented surge during the pandemic, and the rising demand for online goods and services has led to the proliferation of organized retail theft. Federal law carries particularly strict penalties for these types of crimes. To strengthen responses to cyber offenses, law enforcement and criminal defense investigations require computer forensic experts who are experienced at recovering digital evidence. But between increasingly advanced technology and the internet's intrinsic anonymity, many white-collar cybercrimes are unidentifiable.[21] Because white-collar cybercrime is a relatively new concept in criminal justice, few studies have been done regarding the impact of technology on white-collar crime and what elicits white-collar behavior.

Forced Interoperability

Congress has drafted interoperability requirements for online platforms, requiring them to open their services through application programming interfaces (APIs) in an effort to increase competition. Although this legislation has not been passed, it indicates the potential for new regulatory mandates in the industry. Some cyber professionals are concerned that interoperability may enable undesirable stakeholders or organizations to gain access to communities they otherwise could not reach.[22] A major challenge will be managing and securing integrated security products and systems that are unable or not designed to communicate with each other. However, integration can promote common standards that may increase the stability of cyber infrastructure.[23]

Ineffective, Unactionable Information Sharing

Cross-sector collaboration via proactive information-sharing is increasingly important to building national resilience to cyberattacks. Some well-known existing cyber threat intelligence reporting mechanisms include the Structured Threat Information Expression (STIX™) and MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) frameworks. Companies looking for more industry-specific information-sharing, known as Industry Sharing and Analysis Centers (ISACs), are commonplace. Between government institutions and companies, issues that often hinder successful information-sharing is the timeliness, relevance, and complexity of the data reported. For instance, CISA is a starting point for facilitating better industry collaboration, but the quality of information shared with their Automated Indicator Sharing (AIS) participants is not always actionable or contains enough adequate information to be helpful.[24] As a result, these communication breakdowns have led to exploited vulnerabilities or false alarms.

Social Engineering

Social engineering attacks use psychology to manipulate people into sharing sensitive information or granting access to systems. It is less of a cyberattack and more of a confidence game where millions of people around the world are deceived and fall victim to scams. Many fraudsters target senior citizens who may have limited cybersecurity awareness. Attacks happen frequently enough to merit special consideration and training. In recent years these attacks have become more targeted, sophisticated, and abundant due to the profusion of online information on individuals of interest. Cybersecurity professionals are uniquely aware of the dangers as these attacks create unwitting insiders who operate on behalf of cybercriminals.

Cryptocurrency as a Monetization Tool

Cryptocurrency has seen a dramatic uptick in use in the last few years, with bitcoin becoming mainstream and merchants increasingly accepting it as a form of payment. But it is also highly prevalent in use for criminal activity. The bitcoins are easy to transfer and store, can be bought and sold anonymously anywhere in the world, and their transactions are permanent. In their ransomware transactions, most hackers require payment in bitcoins, and the currency is also used for transactions over the dark web.[25] Nevertheless, illicit activities represent a tiny fraction of cryptocurrency use, and law enforcement can trace crypto criminals and even recover funds. Although, certain kinds of crypto bake in more privacy and decentralization, making identifications more difficult. But cybercrime is also prevalent within cryptocurrency itself. Crypto fraud has skyrocketed in the last couple of years, with $14 billion being sent to illegal addresses in 2021.[26] With the increased flexibility that comes with cryptocurrency as a payment for cybercrime, it limits the ability of authorities to track and seize assets stemming from these activities.

Commercial Surveillance

The availability of commercial products that can track and monitor individuals' activities presents a unique threat to privacy and cybersecurity systems. These off-the-shelf products include both physical and digital tracking. Nefarious actors can use commercially available products to spy and gain access or information. In addition, the magnitude of products available makes it difficult to regulate and control who uses them. A well-known example of this is the Pegasus tool, which can be used to access everything on mobile devices. Last year, the U.S. government issued warnings about this and similar tools.

Cookie Theft

Cookie theft is a type of man-in-the-middle attack that captures a user's cookie (browser-based information) to take over the user's accounts. This information might include a username, password or session ID associated with the particular login. This occurs most often on public, shared Wi-Fi networks but can also be captured through malware installed directly on machines or cross-site scripting (analogous to SQL injections). There are several ways for cookie theft to occur, but they all amount to a user's browser data unknowingly being hijacked. The Russian Foreign Intelligence is known to use cookie theft to evade multifactor authentication.

Identity Proofing

Identity proofing is used both at account opening and account recovery, such as when someone loses a password or other authenticator. It generally involves verifying digital data such as biometrics, credit report data, or scans or photos of government-issued credentials. It is most relevant for systems in which distinguishing users is critical, such as financial services, health, or government services. A significant challenge is that adversaries have caught up with many commonly used remote identity proofing tools, enabling them to steal or spoof identities, leading to billions of dollars in losses. More secure tools are needed, including ones that can close the gap between credentials that are commonly used for in-person identity proofing, such as a driver's license or passport, and the lack of secure digital counterparts to those credentials that can be used online. The National Institute of Standards and Technology's Digital Identity Guidelines detail a spectrum of identity assurance levels, ranging from no validation to in-person identity verification.[27]

Reliance on Open Source Software

A community of volunteers often develop open source software, working together to improve the software and share their modifications with others. In cybersecurity, it allows users to examine source code and identify any vulnerabilities that exist. On the other hand, when a bug is discovered, it affects all the systems that have incorporated the code. Another potential issue arises if developers do not actively maintain the open source software, leading to vulnerabilities that go unpatched. It can also be difficult to track who is responsible for any given component of open source software and who is responsible from addressing security issues that arise. Finally, open source software can sometimes be a way to distribute malware or other malicious software. This can occur if someone with malicious intent modifies the open source code and distributes it to others.

Insider Threats, Extortion, Trust Without Verification

CISA identifies four types of insider threats, or security breaches initiated by those within an organization: Unintentional (including negligent and accidental), intentional, collusive, and third party.[28] Beyond the types of insider threat that exists, different kinds of collaboration operations can add to the risks of insider collusion. These types of operations lead to extortion of capital, sensitive information, or proprietary data and can harm public- and private-sector organizations. Trust Without Verification is when an insider or a compromised trusted employee uses his or her access to 1) spread misinformation, malware, or phishing scams, or 2) to gain access to systems that would otherwise require heightened user permissions. Insider threats are difficult to detect or prevent, as the fact that they operate from inside the organization renders most security measures such as firewalls ineffective.

Malware Commercialization

Many criminals are turning to malware as a Service and Ransomware as a Service (RaaS) for their hacking needs, and it is easier than ever to find these programs on the dark web. These software kits allow criminals to franchise or rent their attack software to affiliates. Many vendors even provide tutorials on how to use their software, so the technical proficiency of the user can be minimal. Some examples of RaaS kits include Locky, Goliath, Shark, Stampado, Encryptor, and Jokeroo, but vendors are often disappearing to retool and enhance their business models. This presents a unique challenge for cyber professionals as the barrier to entry for launching an attack is substantially lowered with this model.

Favoring Built-In App Security vs. Bolt-On

The argument of building a cyber culture with security at the forefront would suggest that companies and others must build security into the tech development process, rather than considering it afterward. However, the need can depend on what particular features a built-in or bolt-on system provides, and how crucial they are for a given application. The answer may well differ for IT versus OT. Built-in can take longer and be more expensive than bolt-on, but given the recent increased emphasis on cybersecurity, this might be less of an issue than before. The practice of building in cybersecurity requires a number of organizational and cultural practices, and the aim is to ensure a holistic, integrated approach.

Ineffective/Erosion of Foundational Controls

Foundational controls refer to the basic security measures that form the basis for an organization's overall security posture. This includes access controls, passwords, and network security measures. Over time these controls need to be regularly assessed to ensure they remain effective at protecting against

cyber threats. For example, if an organization required a password to access its email, the rules for selecting a password should be changed to ensure the level of complexity needed to beat brute-force attacks. This practice is now being updated to require multifactor authorization to keep up with even more complex threats. While foundational controls are complex enough of an issue for computer systems, operational technology faces even more of a challenge in updates to their systems.

Compromised Credentials

For years, the dangers with compromised credentials were limited largely to passwords, but in recent years, adversaries have figured out how to compromise some multifactor authentication (MFA) tools as well. Traditional attacks on passwords focused on brute-force attacks, and "credential stuffing" has now been augmented by more sophisticated phishing attacks that not only trick users into handing over even the most complex of passwords, but also the one-time passcodes (OTPs) that are used as a second factor to protect accounts. Adversaries have also found ways to phish MFA based on responses to push notifications, and this new breach has been used in several high-profile attacks. CISA and the National Institute of Standards and Technology (NIST) now advise organizations to use not just any multifactor authentication but multifactor authentication that is designed to be "phishing resistant," such as MFA using the Fast Identify Online Authentication (FIDO) standards.

Data Decryption

Data encryption is incredibly important in cybersecurity and plays a critical role in protecting privacy online, storing data, and securing network data transfers. Many users assume that if they encrypt their data (or get a notification that it has been encrypted), it will be safe. Unfortunately, some encryption algorithms have been broken or have small description keys that can be brute-forced open. As researchers crack encryption algorithms, systems must be updated with newer or more sophisticated encryption codes.

On the other side of the issue, companies are facing increasing pressure to provide access to encrypted data. Criminals and hackers can easily hide their actions using encryption. Ransomware attacks often include an encryption component – victims only receive access to encrypted files once they pay and are given a key. Governments argue that they need access to encrypted communications and files for the safety of their citizens. If the industry succumbs to this pressure, all encryptions could be at risk because more actors can access the keys or processes to decrypt files. In the long term, some technologists are not confident in encryption over the long run due to quantum computing.

Appendix

Formation of the Working Group

Over the course of several months, the co-chairs of this working group identified cyber leaders from strategically important industries, civil society, government, and utility sectors. We reached out to every sector of the economy and level of government that has a stake in cybersecurity, including banking, communications, digital platforms, health, and energy. Furthermore, we felt strongly that stakeholders representing privacy concerns and digital identities needed to be represented in the working group. The group's membership, as a result, encompasses the diverse set of concerns in the cybersecurity space.

Process for Identifying Key Threats

The eight risks identified in part one of this report represent a concentrated effort by the working group to prioritize what it considered to be the most probable and impactful for 2023. At the start of this initiative, we held two brainstorming sessions in which our group identified as many risks as it could. Considering the wealth of experience, knowledge, and diversity of the group members, we came up with a robust list of risks. A complete review of this initial brainstorming session is available under "Other Notable Risks," organized into strategic-level risks and operational-level threats.

After collecting and organizing the brainstormed risks, we met again to consolidate the list by asking each member to identify which risks had the highest probability for 2023. We consolidated from 60 risks to 8 risks over two meetings to finalize the top risks for 2023 documented in this report.

Assumptions about 2023 Threats

In considering these risks and prioritizing which were the most pressing, the working group made several assumptions based on current events. Given the dynamic nature of cybersecurity, some of these risks may be subsumed by real-world events as they unfold. Others could be prioritized by cyber professionals and addressed without major incidents. Our hope is that this list informs and prepares the United States for the year and that at least some, if not all, are addressed without incident. Major assumptions for this report include:

- The current geopolitical landscape and nation-state actors remain consistent;
- No major new technologies are deployed that would affect the U.S. cybersecurity apparatus;
- Policymakers continue 2022 policy priorities, and cybersecurity is not politicized.

Continued Work

This report is a culmination of months of deliberation about the current and potential threats facing the United States in 2023. As the year progresses, BPC will continue to cover the risks laid out in the report and will hope to engage policymakers, stakeholders, and experts as we look to further contribute ideas on a complex and important issue.

Endnotes

1 Dan Lohrmann, "Cyber Attacks Against Critical Infrastructure Quietly Increase," *Government Technology*, July 31, 2022. Available at: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/cyber-attacks-against-critical-infrastructure-quietly-increase.

2 "DOD Cybersecurity: Enhanced Attention Needed to Ensure Cyber Incidents are Appropriately Reported and Shared," U.S. Government Accountability Office, November 14, 2022. Available at: https://www.gao.gov/products/gao-23-105084.

3 Knut Alick, Ed Barriball, and Vera Trautwein, "How COVID-19 is reshaping supply chains," McKinsey & Company, November 23, 2021. Available at: https://www.mckinsey.com/capabilities/operations/our-insights/how-covid-19-is-reshaping-supply-chains.

4 Bill Conerly, "Interest Rates Going Up Even More in 2023," *Forbes*, November 10, 2022. Available at: https://www.forbes.com/sites/billconerly/2022/11/10/interest-rates-going-up-even-more-in-2023/.

5 *IC3 2009 Annual Report on Internet Crime Released,* FBI. National White Collar Crime Center, March 12, 2010. Available at: https://archives.fbi.gov/archives/news/pressrel/press-releases/ic3-2009-annual-report-on-internet-crime-released.

6 Phyllis Sumner, Jonathan Day, and Michael Mahoney, "Cybersecurity: An Evolving Governance Challenge," Harvard Law School Forum on Corporate Governance, March 15, 2022. Available at: https://corpgov.law.harvard.edu/2020/03/15/cybersecurity-an-evolving-governance-challenge/.

7 Chuck Seets and Pat Niemann, "How cyber governance and disclosures are closing the gaps in 2022," Harvard Law School Forum on Corporate Governance, October 2, 2022. Available at: https://corpgov.law.harvard.edu/2022/10/02/how-cyber-governance-and-disclosures-are-closing-the-gaps-in-2022/.

8 "Strengthen your cybersecurity," U.S. Small Business Administration. Available at: https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity.

9 The State of Ransomware in the US: Report and Statistics 2022," Emsisoft, January 1, 2023. Available at: https://www.emsisoft.com/en/blog/43258/the-state-of-ransomware-in-the-us-report-and-statistics-2022/.

10 "The Cost and Impact on Patient Safety and Care," Proofpoint. Available at: https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf.

11 "Ponemon Report: Data Risk in the Third-Party Ecosystem Study," RiskRecon. Available at: https://www.riskrecon.com/ponemon-report-data-risk-in-the-third-party-ecosystem-study.

12 "TPRM risk: Third Party Tracker," PwC. Available at: https://www.pwc.com/us/en/tech-effect/cybersecurity/third-party-relationship-risks.html.

13 "2022 Data Breach Investigations Report," Verizon. Available at: https://www.verizon.com/business/resources/reports/dbir/.

14 "A Guide to Critical Infrastructure Security and Resilience," Cybersecurity and Infrastructure Security Agency, November 2019. Available at: https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf.

15 "NSTAC IT-OT Convergence Report_508 Compliant," CISA, August 23, 2022. Available at: https://www.cisa.gov/sites/default/files/publications/NSTAC%20IT-OT%20Convergence%20Report_508%20Compliant_0.pdf.

16 Knut Alick, Ed Barriball, and Vera Trautwein, "How COVID-19 is reshaping supply chains," McKinsey & Company, November 23, 2021. Available at: https://www.mckinsey.com/capabilities/operations/our-insights/how-covid-19-is-reshaping-supply-chains.

17 Sydney Lake, "The cybersecurity industry is short 3.4 million workers—that's good news for cyber wages," *Fortune Education*, October 20, 2022. Available at: https://fortune.com/education/articles/the-cybersecurity-industry-is-short-3-4-million-workers-thats-good-news-for-cyber-wages/.

18 Anne Boustead, Christos Makridis, and Scott Shackelford, "Defining 'Reasonable' Cybersecurity: Lessons from the States," September 7, 2021. Available at: https://ssrn.com/abstract=3919275.

19 Mike Mclean, "2022 Must-Know Cyber Attack Statistics and Trends," Embroker, December 7, 2022. Available at: https://www.embroker.com/blog/cyber-attack-statistics/.

20 "Cost of a data breach 2022," IBM. Available at: https://www.ibm.com/reports/data-breach.

21 Brian Payne, "White-Collar Cybercrime: White-Collar Crime, Cybercrime, or Both?" *Criminology, Criminal Justice, Law & Society* 19(3): 16–32, 2018. Available at: https://ccjls.scholasticahq.com/article/6329-white-collar-cybercrime-white-collar-crime-cybercrime-or-both.

22 Daniel Castro, "Potential Unintended Consequences for Social Media of Mandatory Interoperability Requirements in Sen. Klobuchar's Tech Reform Bill," Information Technology & Innovation Foundation, January 21, 2022. Available at: https://itif.org/publications/2022/01/21/potential-unintended-consequences-social-media-mandatory-interoperability/.

23 James Lewis, "Cybersecurity and the Problem of Interoperability," Center for Strategic and International Studies. Available at: https://www.csis.org/analysis/cybersecurity-and-problem-interoperability.

24 Joseph Cuffari. "Additional Progress Needed to Improve Information Sharing under the Cybersecurity Act of 2015." Department of Homeland Security: Office of Inspector General. August 16, 2022. Available at: https://www.oig.dhs.gov/reports/2022/additional-progress-needed-improve-information-sharing-under-cybersecurity-act-2015/oig-22-59-aug22.

25 "Why Do Hackers Use Bitcoin? And Other Cybersecurity Questions Answered," ECPI University. Available at: https://www.ecpi.edu/blog/why-do-hackers-use-bitcoin-and-other-cybersecurity-questions-answered.

26 Gertrude Chavez-Dreyfuss, "Cryptocurrency crime in 2021 hits all-time high in value -Chainalysis," Reuters, January 6, 2022. Available at: https://www.reuters.com/markets/us/cryptocurrency-crime-2021-hits-all-time-high-value-chainalysis-2022-01-06/.

27 Paul Grassi, James Fenton, et al., *Review of Digital Identity Guidelines: Enrollment and Identity Proofing*, U.S. Department of Commerce, National Institute of Standards and Technology, June 2017. Available at: https://csrc.nist.gov/publications/detail/sp/800-63a/final.

28 "Defining Insider Threats," CISA. Available at: https://www.cisa.gov/defining-insider-threats.

1225 Eye St NW, Suite 1000
Washington, DC 20005

bipartisanpolicy.org

202 - 204 - 2400

The Bipartisan Policy Center (BPC) is a Washington, D.C.-based think tank that actively fosters bipartisanship by combining the best ideas from both parties to promote health, security, and opportunity for all Americans. Our policy solutions are the product of informed deliberations by former elected and appointed officials, business and labor leaders, and academics and advocates who represent both ends of the political spectrum.

BPC prioritizes one thing above all else: getting things done.

@BPC_Bipartisan
facebook.com/BipartisanPolicyCenter
instagram.com/BPC_Bipartisan

Policy Areas

Campus Free Expression

Economy

Education

Energy

Governance

Health

Immigration

Infrastructure

IDEAS
ACTION
RESULTS

Bipartisan Policy Center

1225 Eye Street NW, Suite 1000
Washington, D.C. 20005