The Global Cyberwar and Societal Response

by Raymond Hutchins and Mitch Tanenbaum

Last update: Jun. 27, 2025

This non-technical report describes how governments are being forced into ever more proscriptive cybersecurity and privacy regulations and how business leaders must improve governance to reduce risks and enhance corporate valuations.

AI Statement: This document was written by a human being ***and not AI***. While we may use AI for aspects of our research, we find that AI is (thus far) incapable of writing a document of this kind.

Contents

1.0 The Global Cyberwar and the Cost to Society

NOTE: What follows is a front-line report on the global "cyber war" as seen by cybersecurity professionals actively engaged in the mission of protecting the U.S. financial system and Department of Defense (DoD) assets. This report is intended to serve as a reference document for you. Please retain and share with others who might benefit from understanding this strategic, non-technical analysis.

1.1 What Cyberwar?

Our country, financial systems, defense capabilities, money, and our citizens are under active assault from a bewildering array of adversaries and criminals, both foreign and domestic. Considering the involvement of various national governments, it is reasonable to describe what is going on as "war." Even though this is an undeclared war, the risks to nations are real.

Business leaders may intuitively grasp this situation, but very few *act* like they are in a war-like environment even though their businesses and systems are directly threatened. Based on our front-line observations, this "head-in-the-sand" behavior occurs because these leaders don't understand the war or the risks–it's like nothing they have ever seen before. This is despite the fact that news of new breaches surfaces daily. Until business leaders discover *they* have been breached; most leaders won't start quantifying or responding to the risks.

Today's reality is that all digital societies are fearfully dependent upon their IT infrastructures and the software and electrical energy that powers them. These global IT infrastructures are rapidly expanding via the *Internet of Things* (IoT). Anything connected to the Internet can be hacked. Almost everything is being connected to the Internet. As a result, everything is becoming vulnerable this cyberwar.

There's more.

New digital technologies such as quantum computing, AI, and crypto currencies may pose risks that outweigh their benefits. (Please see 8.0-*The Impact of New Technologies*).

Many nations, and even criminal syndicates, are now capable of destroying part (or even all) of the IT and power infrastructures of other countries. These capabilities are threats to our very social order.

And beyond countries and criminal organizations, individuals with smarts and internet access can wreak havoc. While we typically look abroad for our adversaries, when it comes to cybercrime, the U.S. is a virtual hotbed of criminals and insiders engaged in corporate espionage, theft, and fraud.

Beyond external adversaries, a significant and often more insidious threat in the cyberwar comes from within organizations: insider threats. These threats can be either malicious or unintentional, but both pose serious risks to an organization's security. Malicious insiders, in

particular, are increasingly recognized as a greater systemic risk to Western democracies than traditional cyberattacks or conventional espionage.

Insider threats are uniquely dangerous because they can bypass traditional perimeter defenses and often involve extended "dwell times" (an average of 11 months compared to 3 days for external breaches). They frequently involve the use of legitimate credentials, making forensic attribution extremely challenging. Common scenarios include former employees retaining active credentials, intellectual property theft by transitioning employees (sometimes driven by corporate espionage acting as a proxy for state-sponsored intelligence gathering), unintentional data exposure through personal devices, and revenge-motivated data leaks by disgruntled staff. Organizations often focus primarily on external threats, underestimating the risks posed by internal actors, which makes early detection difficult.

Mitigating insider threats requires a comprehensive Insider Threat Program (ITP) that integrates technical, procedural, and cultural components. Key practices include strengthening onboarding and offboarding policies (especially for access revocation), implementing strict access controls (like the principle of least privilege), enforcing data classification and monitoring, educating employees on data ownership, monitoring high-risk users, regularly auditing access logs, and establishing a dedicated insider threat management team.

They are the enemy within, and they have nothing to fear. This is the golden age of cybercrime. The odds of being caught are nil.

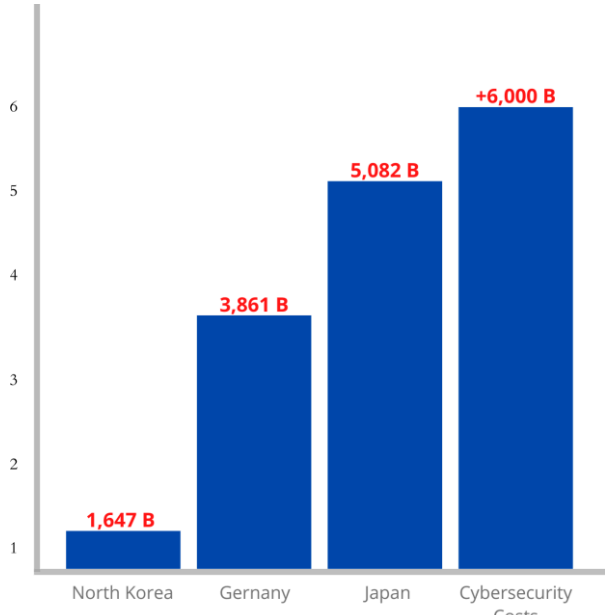
Sadly, cyberwar is real and unlike other weapons of mass destruction (nuclear, biological, and chemical) …no treaties govern it. It's the Wild West all over again–and the criminals are free to roam. Unlike nuclear weapons, cyber weapons do not require billions in infrastructure to deliver their payload. Just one person who clicks on the wrong thing can open the door and expose an entire organization.

One last point. It can be said that a war is when *everyone* puts up a fight. As front-line soldiers inthis war, we are reporting that, in this war, our side is not putting up the fight it should.

> *"The range of criminal, cyber and counterintelligence threats we face as a nation has never been greater or more diverse."* --FBI Director Christopher Wray, testifying before a Senate Appropriations subcommittee, May 25, 2022

1.2 What Are the Losses?

Historically, costs and losses associated with global cybercrime and the cyberwar have been notoriously underestimated. When you consider the fact that multiple nations have organized cyber armies for military and economic warfare against their adversaries, and that most crimes still go unreported, it is understandable why it is so difficult to calculate losses.



While global theft, fraud, and other *direct* financial losses are huge, it is even harder to assess and calculate the loss of business, scientific, academic, engineering, and military *intellectual property*.

In 2019, then-Defense Secretary Mark Esper warned that China was perpetrating the "greatest intellectual property theft in human history," just days after retired Navy Adm. William McRaven said that China's growing technological capabilities should be a "holy s--- moment" for the US.[1] Since then, China's 300,000-strong cyber army has not backed off its efforts.

A recent *Boardroom Cybersecurity 2022 Report*[2] calculated global 2022 losses at $7 trillion. To put this kind of loss into context, it may be useful to note the annual GDP of the top three countries: USA ($20.4 trillion), China ($13.4 trillion), Japan: ($5.0 trillion).

So, what is the value of having a country's entire population's personal data stolen by adversaries? Questions that business and political leaders must ask now are:

1
2 https://www.businessinsider.com/esper-warning-china-intellectual-property-theft-greatest-in-history-2019-9
https://www.einnews.com/pr_news/585389499/cybercrime-damages-to-cost-the-world-7-trillion-usd-in-2022

- How much money is being fraudulently removed from our economy?
- Where is that money going?
- Into which banks in which countries?
- How complicit are global governments and banks in this illegal transfer of wealth?
- How can the integrity and credibility of financial systems and markets be maintained with such systemic criminality, corruption, and huge losses?
- At what point does the system break?

2.0 Why Governments Are Being Forced to Act

Thus far in the history of the global cybersecurity crisis, government, scientific, military, and business leadership has been slow to act. There are many reasons for this, but some higher-level reasons include:

- The rapidity of the digital revolution and the huge movement of data into IT infrastructures that were never designed for security.
- Most legislators are older and have not truly experienced our budding digital age. Their lack of understanding and experience with technology makes for very slow progress.
- The newness, complexity, and speed of cybersecurity and privacy threats.
- The mind-blowingly fast arrival of IoT, quantum computing, artificial intelligence, and crypto currencies.
- Resistance to new regulations and laws by businesses and non-governmental organizations that is basically caused by a lack of trust.

- The shortage of trained, experienced business and governmental leaders in regard to IT, cybersecurity, and privacy issues.
- The upfront expense and loss of productivity associated with protecting data.

While legislatures may be still catching up, various U.S. federal agencies[3] have been in the battle for some time. These agencies include:

- Cybersecurity and Infrastructure Security Agency (CISA)
- U.S. Department of Homeland Security (DHS)
- National Cybersecurity and Communications Integration Center (NCCIC)
- Office of Cybersecurity and Communications (CS&C)
- United States Secret Service (USSS)
- FBI Internet Cyber Crimes Center (iC3)
- U.S. Department of Justice (DOJ)
- Federal Bureau of Investigation (FBI)
- National Cyber Investigative Joint Task Force (NCIJTF)
- National Security Cyber Specialist (NSCS) network
- National Security Division (NSD)
- NSA-National Security Cyber Assistance Program (NSCAP)
- DoD-U.S. Cyber Command
- SEC Crypto Assets and Cyber Unit

While this array of agencies has still not come close to solving the problem, their front-line work has allowed them to better see what's going on and has clearly established the threat to our country, and these agencies have been communicating the urgency of the issue to federal and state leaders.

[3] https://voxglobal.com/intersection/2015/02/the-cybersecurity-efforts-of-federal-agencies-101/

This (and huge losses across society) explain why governments are starting to move with more urgency.

According to Harvard Business Review[4] ,cybersecurity has reached a tipping point. After decades of all governments basically taking a hands-off approach to cybersecurity, national, state and even local governments are starting to move. Some have implemented (and many more are considering)new laws governing cybersecurity and privacy.

But even though lawmakers feel a need to do something, they often struggle to regulate technology for the reasons described above.

Laws and regulations are being made at both the federal and state levels. Some are industry specific while others affect everyone. Some have exemptions for different classes of people and organizations, while others don't.

It is important for businesses–specifically their executives and board members (the people responsible for controlling risk)–to understand this changing landscape. They must now do what they have not yet done…*accept their responsibilities and duties to protect data, reduce risk, and enhance valuations.*

2.0 Industry Standards that Address the Cyberwar

When governments build cybersecurity and/or privacy legislation/regulations, they typically look to established industry standards for guidance about best practices. While not perfect (for example,

none cover work-from-anywhere yet), they are typically quite good and thorough.

The standards which currently dominate are:

- Europe cyber: The International Standards Organization (ISO) 27000 standard family.[5]
- Europe privacy: The General Data Protection Regulation (GDPR)
- U.S. cyber: the National Institute of Standards (NIST) Cybersecurity Framework (CF) and the Secure Software Development Framework (SSDF)
- U.S. privacy: The NIST Privacy Framework (PF)

NOTE: The U.S. DoD has built its compliance standards upon the NIST standard. (See 6.1 below)

3.0 Cybersecurity Laws and Regulations

There exists a bewildering array of cybersecurity laws internationally and in the U.S. For U.S. companies doing business nationally or internationally, this complicates compliance. Until the United Nations can implement an international law or treaty regulating cyberspace, the various countries of the world are left to their own devices.

While enforcement of many of these laws is currently spotty and is complicated by the fact that enforcement agencies are under-resourced, if one fails to perform their responsibilities with respect to cybersecurity, the legal justification to drop the hammer exists–and enforcement agencies are looking to make examples. We are seeing this at both the national, state, and local levels.

Wikipedia offers a reasonable summary of current and proposed U.S. and international cybersecurity regulations and laws.[6]

You'll note that the European Union has made serious progress implementing *national* (in their case…*continental*) cybersecurity and privacy legislation–something the rest of the world has not been able to do.

In a perfect world, the U.S. would have a single, national law addressing privacy and security, but the U.S. legal system is not perfect. As a result, the individual states have begun addressing this issue and, as of the time this paper was written, all fifty states have some form of cybersecurity law. Most states have a first- generation privacy law, and five states have a second-generation privacy law. (See 4.4 below for more information)

4.0 Privacy Laws and Regulations

4.1 New Rights for *Some* People on Earth

Led by the European Union, liberal democracies are attempting to grant new data and privacy rights to their citizens. Authoritarian governments, led by China, are going in the exact opposite direction, taking away all data and privacy rights of their citizens.

It is an open question as to whether the U.S. Constitution gives people a right to privacy. The

Fourth Amendment protects against unreasonable searches, but that was written before the age of the computer and the Internet. U.S. courts (including the Supreme Court) are not quite sure if there is a fundamental right to privacy and personal data ownership.

Possible rights include: (1) the right to obtain a copy of data that a company has collected about you or (2) the right to correct incorrect data that a company has collected or (3) the right to demand that a company delete your data from its IT infrastructure. As we will see later, those rights are separate, and a law might grant one of them without the other/s.

The bottom line is that until around 2016, no laws anywhere in the world addressed these issues, and since they address fundamental (and new) human rights, we will go into a bit of detail.

4.2 International Privacy Laws

According to the United Nations, 137 out of 194 countries have put in place legislation to secure the protection of data and privacy for its citizens.[7] While there may be some formal attempt to put legislation in place, even in developed countries, the state of enforcement is such that no such protections actually exist. And as mentioned earlier, in countries with authoritarian regimes, there is no sign the citizens will ever have these rights.
The European Union's General Data Protection Regulation (GDPR) was adopted in 2016 and went into effect on May 25, 2018. This piece of legislation is the model for legislation occurring in the U.S. and around the world.

[4] https://hbr.org/2022/08/new-cybersecurity-regulations-are-coming-heres-how-to-prepare

[5] https://www.iso.org/standard/73906.html

7 https://en.wikipedia.org/wiki/Cyber-security_regulation
https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

4.3 U.S. Federal Privacy Legislation

While some large tech companies and others have supported a U.S. federal privacy law that supersedes those implemented by individual states, thus far, there is no serious movement towards such a law. State legislators and their citizens seem disinclined to forgo the new data privacy rightsthey have been granted.

American Data Privacy and Protection Act (ADPPA)

The ADPPA is the most recent attempt at nuking state privacy laws via federal legislation. There are many people who do not like California's law (see below), which includes a private right of action to sue in case of a breach. While some people said this new right would cause an avalancheof lawsuits, the reality is quite different. This appears to be because contingency privacy lawsuits are extremely difficult to pursue, and most are thrown out. Thus far, there is little economic incentive for lawyers to pursue such cases.

Given the politics of Washington, we rate the likelihood of the ADPPA passing as low–at least fornow.

4.4 U.S. State Privacy Legislation - California Leading the Charge

California led the nation in creating the first cybersecurity law, CA SB 1386 (notice the immediate connection between cybersecurity and privacy–see more below). Passed in 2002, it was considered radical at the time. It said that businesses had a duty to protect consumers' information. It also made an attempt to define what information needed to be protected. It did not give consumers any rights in their data, and it made the Attorney General responsible for enforcement.

Since the AG has a lot of laws to be responsible for and since the law did not give the AG any more money or people to enforce it, only the most egregious violations were ever prosecuted. In the next almost 20 years, every state implemented a law, mostly based on CA SB 1386. The details changed. What data needed to be protected changed. What you had to do in case of a breach changed. But the basis for all these laws was CA SB 1386.

4.4 First-Generation and Second-Generation Privacy Laws

Most states have had "first-generation" privacy laws on the books for some time. These laws (loosely) don't offer consumers many protections. Second-generation privacy laws originated in Europe with GDPR and were followed, after several years, by the California Consumer Privacy Act(CCPA). That act is in effect now. CCPA was somewhat of a shotgun wedding to avoid a stronger ballot initiative, but it has gotten watered down by the legislature a bit since it was enacted in 2018. As a result, the California Privacy Rights Act (CPRA) ballot measure was passed in 2020 by California residents. CPRA says (in the law) that the legislature may only strengthen the law by modifying it.

Now California is leading the nation again–for better or worse. They implemented the first second- generation privacy law, and other states are modeling their second-generation laws on California's laws. We say *laws* because there are actually two laws that are relevant–CCPA andCPRA.

The benefit of states creating their own privacy laws is that hopefully they are more agile than the

feds and they can modify their laws more quickly in case mistakes are made.

4.5 Elements of Second-Generation State Privacy Laws

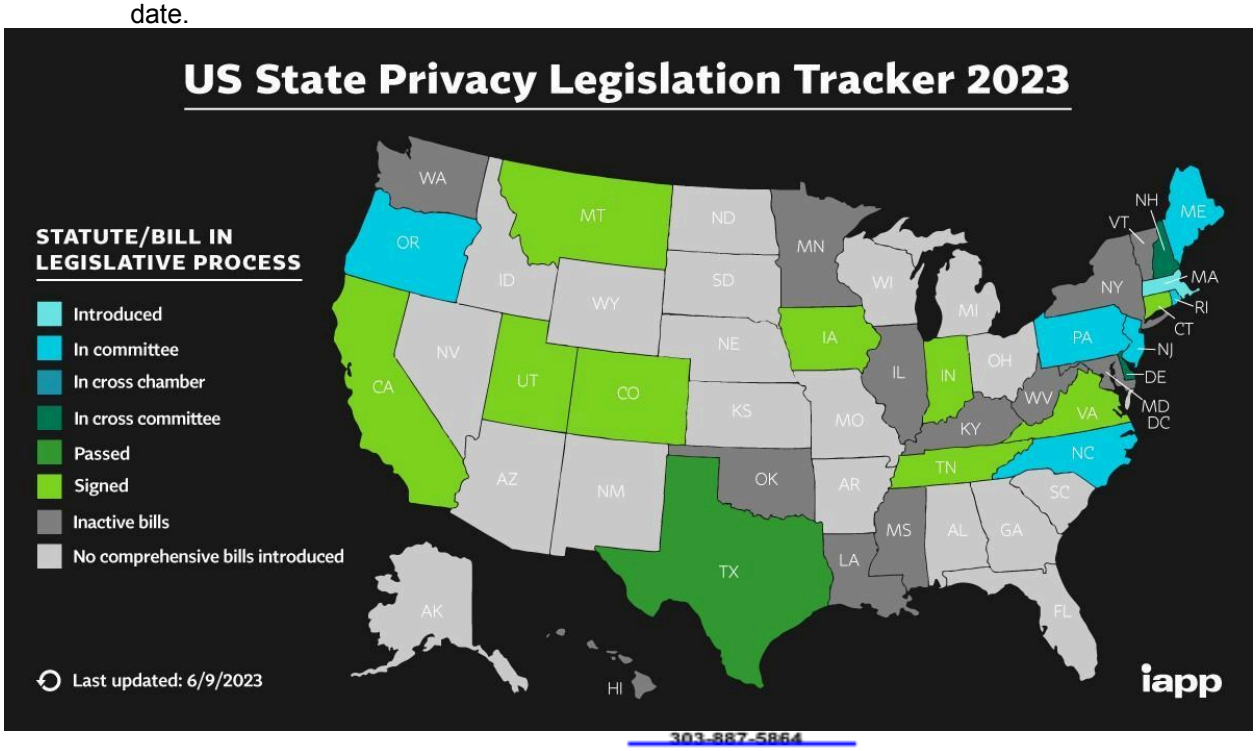
Like GDPR in Europe, second-generation (U.S.) privacy laws create privacy "rights." This is because there is no agreed-to right-to-privacy in the U.S. Constitution, unlike in the E.U. Constitution. Given that the Constitution was created long before the Internet, the founders didn't consider privacy to be a problem. While the rights vary from state to state and hence why businesses would prefer a federal law with state law preemption, here are the rights offered by state privacy laws:

- The consumer's right to obtain a copy of his/her data (free of charge with some restrictions).
- The right to correct the data that was collected.
- The right to have that data deleted (again, with some restrictions).
- The right to stop anyone from sharing that data (loosely, selling it) with others (again, with some restrictions).

Business responsibilities in second-gen laws:

- A simple-language, publicly-posted, privacy policy.
- Businesses must disclose for what purpose(s) they will be using the data collected.
- They must disclose the classes of (and in some cases) the names of the people with whom they are sharing that data.
- They must provide one or more methods for people to take advantage of these rights.
- In some cases, this includes data that is collected in brick-and-mortar locations.
- They must respond quickly to a consumer request (typically no more than 30 days).
- In many cases, these consumer rights trickle down to third parties with whom the consumer'sdata is shared.

Currently, there are twelve states that have passed state privacy laws, with seven more working on laws. The graphic below, outlines the current state law situation. This is a very rapidly changing landscape. Even though this IAPP graphic was recently updated, it is already out of date.



303-887-5864

Note that the velocity of privacy law passage has increased greatly. At the rate we are going now, all 50 states will have laws within 5-10 years.

Several states' laws, including California, Colorado, Connecticut and Virginia are already in effect as of July 1, 2023; the remaining laws become effective in 2024 and 2025. Note that California has two new second- generation laws, both of which are in effect now.. We have created charts that document the details of each of these laws. Here is a snapshot of what those charts look like.

	California	Virginia	Colorado	Utah	Connecticut
Scope	Applies to businesses that: Have $25 million in annual gross revenue **-OR-** Process data of at least 100,000 consumers -or- Derive at least 50% of gross revenues from *selling or sharing* data	Applies to businesses that: Process data of at least 100,000 consumers -or- Process data of at least 25,000 consumers and derive at least 50% of gross revenues from *selling* data	Applies to businesses that: Process data of at least 100,000 consumers -or- Process data of at least 25,000 consumers and derive *revenue or receive a discount on goods or services* from *selling* personal data	Applies to businesses that: Have $25 million in annual gross revenue **-AND-** Process data of at least 100,000 consumers -or- Process data of at least 25,000 consumers and derive at least 50% of gross revenues from *selling* personal data	Applies to businesses that: Process data of at least 100,000 consumers (excluding purely payment transactions) -or- Process data of at least 25,000 consumers and derive at least 50% of gross revenues from *selling* personal data
Effective Date	Jan. 1, 2023	Jan. 1, 2023	July 1, 2023	Dec. 31, 2023	July 1, 2023

The details of each state's law is beyond the scope of this paper, but you can find those details in this shared folder: Shared drives - Google Drive. Note: There are now so many states with privacy laws that we had to break up the document into multiple parts for easy navigation.

Most of the state privacy laws have some minimum business sales volume for compliance, but many of the state cybersecurity laws apply to everyone without exception.

Each state defines which data elements (like a name or driver's license number) are in scope, the definition of sale or sharing of data, what types of organizations are covered, who is exempted (such as health care providers covered by HIPAA), precisely what rights a person has, the responsibilities of covered businesses *and their vendors*, what notices must be provided when, what terms must be written into contracts with service providers, and other items. See the link above to get an idea of these specifics.

In addition, each state will be issuing regulations regarding how businesses must comply. Each state does this differently. California, for example, set up a separate department, the California Privacy Protection Agency, while Colorado, as another example, has charged the Attorney General with creating the regs. What you can count on is many pages of regulations, all different and someconflicting between states.

4.6 Extraterritoriality

Extraterritoriality is a big word that means "my law applies in your jurisdiction." A well-known

example of this is Europe's privacy law, GDPR, which applies to U.S. companies, even to ones that don't have any operations in Europe, but who might possibly have European customers or visitors to their web sites.

In the U.S., states have practiced extraterritoriality since the beginning. State security, breach notification and privacy laws apply to you, whether you have a location in that state or not, if you collect data on a resident of their state. For example, a company located in Texas has to comply with Kansas's cybersecurity and privacy laws, if they collect data on Kansas residents, sell products or services to them, or target them in advertising. Sometimes the nexus is very slight.

4.7 U.S. vs. the European Union

The U.S. and the E.U. have been fighting over adequate privacy for years. The E.U. has an interesting view of the universe wherein the rules the U.S. must play by do not apply to the E.U. As a result, there has been a bit of conflict across the pond. The most recent version of a cross border privacy agreement was struck down by the CJEU, the E.U.'s highest court. European law may allow California to strike a deal with the E.U. regarding adequacy. If they do, then companies based in California, with data stored in California, may be able to transfer data back and forth across the pond freely, while companies elsewhere in the U.S. can't do that. Assuming that happens–and that is a big "if"–then there will be major pressure on the other states and Congress to follow suit so that California companies don't have an unfair advantage over others. This is a big "if," but it could happen.

If you are confused after reading this, you are not alone. Your compliance team has a lot of work ahead of them. Also remember that you must consider that there is a difference between what you are legally required to do and what your customers expect you to do. If your customer, for example, asks for a copy of his or her data and you say, "We are not legally required to provide that" (or some other "get-lost" version of that, odds are that social media will not be your friend. But if you need help sorting this out, please contact us.

How Cybersecurity and Privacy Are Merging

Cybersecurity and privacy laws are both about protecting data within various IT infrastructures. Privacy focuses on personal data of citizens, and cybersecurity focuses on all other valuable data assets. In the short period of time that such security has become an issue, cybersecurity and privacy efforts have been driven by different constituencies. However, since we are talking about protecting data, the conversations are merging.

5.0 How Cybersecurity and Privacy Are Merging

Cybersecurity and privacy laws are both about protecting data within various IT infrastructures. Privacy focuses on personal data of citizens, and cybersecurity focuses on all other valuable data assets. In the short period of time that such security has become an issue, cybersecurity

and privacy efforts have been driven by different constituencies. Since we are talking about protecting data, however, the conversations are merging.

6.0 Societal Response

6.1 Governmental

Throughout this paper are many references to the various U.S. federal and state government efforts to protect the IT infrastructures we all depend upon. Much of the U.S. cyber effort is led by the U.S. Department of Defense (DoD). The DoD's efforts are also impacting our allies around the world, forcing them to be more proactive. (See 6.2 below)

Europe clearly leads the charge on protecting privacy, another category of sensitive data.

While we have seen that all U.S. states have some form of cyber and/or privacy regulations, one state deserves recognition.

DFS 500 or 23 NYCRR 500

Among the U.S. states, New York clearly stands out as the most aggressive cybersecurity legislator and enforcer and deserves special mention. Since 2017, financial institutions and other regulated entities have been required to follow the cybersecurity rules known as DFS 500 or 23 NYCRR 500[8]. This regulation is very specific and proscriptive about what is required, and DFS audits regulated entities using these rules.

This state law is considered "the standard" by other states, which are copying it to one degree or another.

6.2 U.S Department of Defense

A major player in the global cyberwar is the U.S. Department of Defense (DoD).

The DoD has an annual budget of over $800B. It is by far the largest defense budget of any country in the world. Over 300,000 companies (100,000 contractors and their subcontractors) work to supply the DoD with what it needs to protect the country. These companies are referred to as the Defense Industrial Base (DIB).

This amount of money and the number of companies it flows to represent a large part of our economy. It also represents a huge threat to our national security. For these companies to do DoD work, they must have access to sensitive DoD information–and historically, that information has not been protected very well.

It has become apparent that our adversaries have stolen ***hundreds of billions of dollars*** worth of investments in weapon systems and other aspects of our defense efforts. Among other consequences, this theft puts the lives of our military men and women at risk.

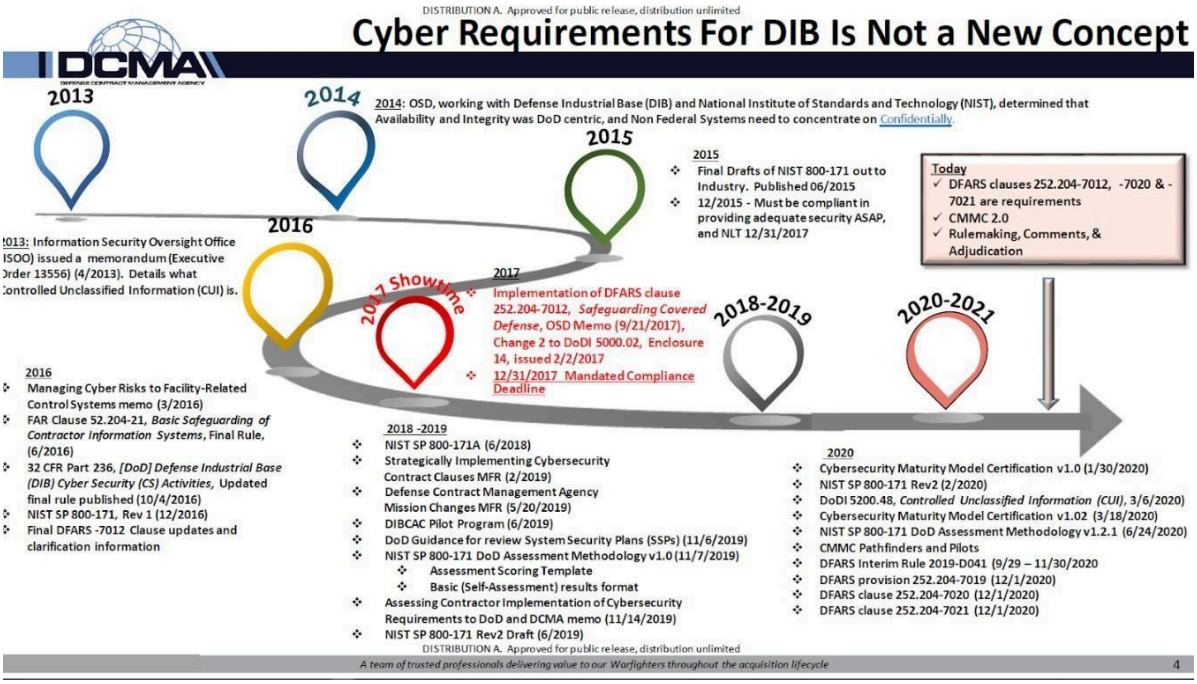
The General Services Administration has been investigating and evaluating these losses, but it is an enormous task.[9] No one is really denying that it has happened, but the question remains–what has been stolen and how do we stop it? And (just as in the civilian sector) it is a tough problem.

The DoD has been working to protect *classified* information stored in DoD's IT infrastructure from

cyber- attack for some time. It also has worked to protect *classified* data stored in the systems of the large DoD "prime contractors," such as Lockheed, Raytheon, Boeing, General Dynamics, and others that play a crucial role in our defense structure. Even with such a focused effort, we read about breaches at organizations like the NSA and CIA on a regular basis. We are hopeful that we have not lost all this information.

But what about those 300,000 companies in the DIB that have access to information which is not classified but which is still very sensitive? This type of DoD data is called *Controlled Unclassified Information* (CUI)[10]. And because it has not been protected, naturally, our adversaries have been having a field day stealing it.

In 2013, the DoD took the first steps to protect such information. In 2015 the DoD started including in the these companies' contracts language that required them to build effective cybersecurity programs (much more info about this below[11]). But until very recently, the DoD did not actively enforce the contract clauses related to cybersecurity. Please also see the timeline below.



Regardless of enforcement, however, the reality (since 2017) is that if a contractor or subcontractor signs a DoD contract and then does not comply with the part that says they must protect the CUI, then that contractor is committing fraud.

Late in 2021, the Department of Justice (DOJ) stood up an enforcement team specifically to pursue DIB companies who lie about their cybersecurity compliance. The team has settled a few cases so far–all with fines in the millions. DOJ plays these things close to the vest, but it is likely they are working on more such enforcement actions. The law they are using allows them to pay whistleblowers up to 30 percent of whatever amount the offender is fined. Recently, one whistleblower was paid $2.61 million[12].

As cybersecurity professionals with decades of DoD experience, we have been challenging the

DoD regarding the weakness of their cyber strategy for years (please see our press release and position paper below[13]). We can report that this new enforcement activity is starting to make a difference.

This DoD enforcement effort has the potential to radically change the cybersecurity posture and capabilities of over 300,000 U.S. companies. It might not solve the problem, but as these companies come into compliance, a great deal of our nation's IT infrastructure will be better protected, and it will be more difficult and expensive for our adversaries (within and without) to threaten us.

[8] https://www.governor.ny.gov/sites/default/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf
[9] https://www.gao.gov/assets/gao-19-128.pdf
[10] https://www.archives.gov/cui
11 https://www.cybercecurity.com/cmmc-assessments/
12 https://www.reuters.com/business/aerospace-defense/aerojet-rocketdyne-pay-9-mln-resolve-allegations-us-cybersecurity-violations-2022-07-08/
13 https://www.einpresswire.com/article/541288336/cybersecurity-professionals-say-dod-cmmc-strategy-will-not-work-suggest-alternate-approach-asap

The DoD enforcement efforts are spreading to other federal agencies. The General Services Administration is already copying the DoD and starting to require cybersecurity compliance in some of its contracts. In addition, several foreign governments are following suit and beginning to implement similar regulations[14]. We anticipate that similar cybersecurity contract requirements will soon be in all major federal contracts, and this will impact more U.S. companies.

Lastly, the DoD actions described above are already having a positive impact on our military allies and those who want to do business with DoD. There is much sharing of cybersecurity information, standards, and processes currently under way between the DoD, the Five Eyes Alliance[15], NATO,and others.

6.3 Corporate Response

A common problem in corporate governance is that often boards of directors just don't do their jobsof making executive management do *their* jobs. Of course, with the advent of the cyberwar, the problem has only gotten worse. Few directors know the first thing about cybersecurity and privacy–not even enough to ask questions of management. But it is hard to hold directors' feet to the fire.

That, however, may be changing.

In 2019 there was a lawsuit that established that members of boards of directors had personal liability for regulatory compliance oversight. This new liability, this new responsibility, is referred to as the *Caremark Standard*.[16]

There is much that boards of directors can do to ensure that management meets its cybersecurity and privacy responsibilities[17]. And since the individual director's personal liability is now on the line, they are more likely to pay more attention to the cyberwar. Naturally, directors would like to shift the risk of cyber liability to the insurance companies who sell them Directors and Officers (D&O) liability insurance. But insurance companies are raising rates and denying coverage to directors and boards that fail to meet their responsibilities for protecting company assets and data.

Additionally, the Federal Trade Commission and the Securities and Exchange Commission are about to drop new rules regarding boards of directors' responsibilities and company data protection requirements.

Hopefully, these changes will improve corporate governance, reduce risk, and increase company valuations.

NOTE: The authors of this paper have produced a short, informative paper on the *Caremark Standard* and how changing the financial incentives for board members would achieve greater risk management behavior from board members. Go HERE to view this paper.

14 https://www.gov.uk/government/publications/industry-security-notices-isns/compliance-with-cyber-security-requirements-from-other-nations
15 https://en.wikipedia.org/wiki/Five_Eyes
16 https://corpgov.law.harvard.edu/2019/07/08/caremark-liability-for-regulatory-compliance-oversight/ 17
https://cybersecurity-training-for-boards.com/

6.4 The Technology Industry

The global technology industry is in a unique position to help fight the cyberwar, but it is hampered by its economic incentives.

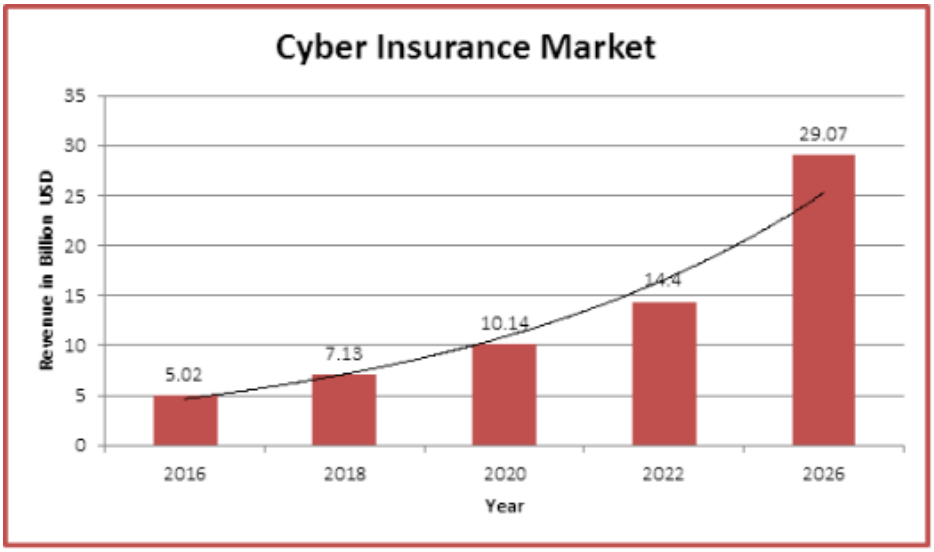
All of us have experienced reading an End User License Agreement (EULA) presented by a technology company as we purchased some type of technology product. Buried in the obtuse and difficult-to-understand language are clauses that shift virtually all risk and responsibility for the use of those technologies to us…the end users. The technology companies already understand the impossibility of their industry assuming responsibility for the security of their hardware and software products. Therefore, they minimize their risk and shift responsibility to the end users.

This represents a deep, systemic flaw in our ability to manage risk. This type of problem can only be addressed by new laws that shift these risks back upon the product manufacturers. This problem represents such a deep and core insecurity in global IT infrastructures, leading edge cybersecurity thinkers and policy makers believe that the problem is unsolvable in the context of "fixing this broken system" and that a new security paradigm is required.[18]

7.0 Additional Players and Variables

7.1 Insurance Industry Pressure

The first cybersecurity insurance policy was written and deployed by AIG in 1997. This was the first time an insurance company started covering this type of business risk. Since then, much has happened in the cybersecurity insurance marketplace.



Initially, cybersecurity insurance companies did not understand this type of risk, but since then, they have learned much. And most businesses that are responsible for protecting data and who must comply with national, or state regulations seek out this type of protection. As a result, the insurance industry is exerting much pressure on businesses to improve their cybersecurity practices.

Insurance companies now closely question cyber insurance customers to determine cybersecurity maturity, and many insurance companies employ technology tools to continuously monitor clients' networks for problems. The old days of lying to the insurance carrier about what you were or weren't doing to meet data and system protection are over. One wrong move and you may find that you have lost your insurance at the very moment you need it the most.

[18] https://www.einpresswire.com/article/541288336/cybersecurity-professionals-say-dod-cmmc-strategy-will-not-work-suggest-alternate-approach-asap

SwissRe provides both primary cyber insurance and re-insurance to insurance companies. They just released some concerning stats. Premiums reached $10 billion last year and they expect that to rise to $23 billion by 2025. Annual cyberattack losses reached $945 billion globally and about 90 percent of that is *uninsured*.
Forrester says the typical breach costs $2.4 million, but less than 20 percent of companies have more than $600k in coverage. SwissRe has made a number of recommendations, including standards to get coverage and even a government-backed fund to address the gaps. Read the full article here.[19]

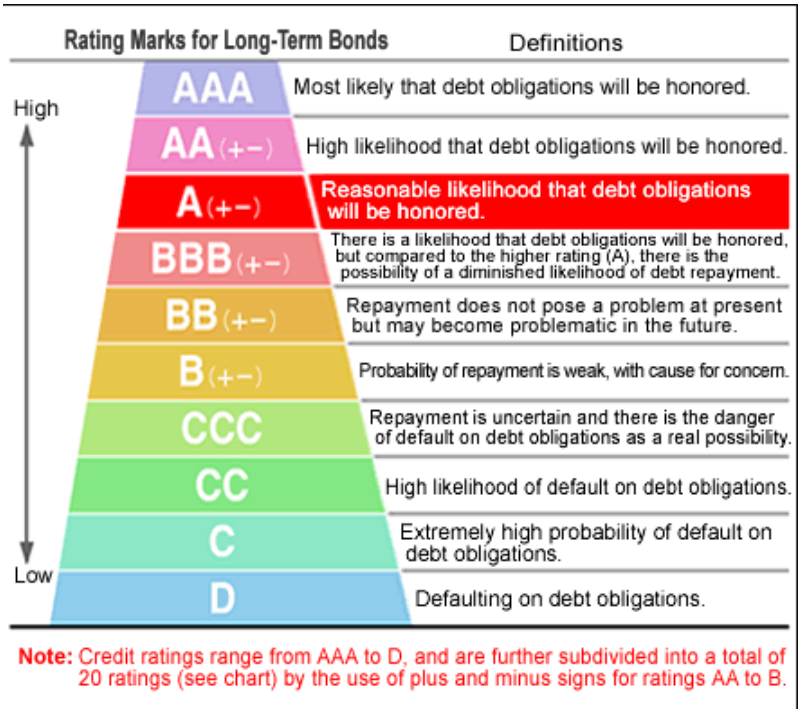
Here is another article that goes into more depth on this important topic:
https://www.chicagofed.org/publications/chicago-fed-letter/2019/426

While we have observed that the insurance industry and their lawyers have gotten much better at crafting insurance policies that protect *their* interests, most business leaders are not able to decipher their policies to determine if they have the correct coverage.

NOTE: The use of a company such as ours to assist in a cyber insurance policy review can be a very wise decision that pays off at a critical moment. See below:

Cyber insurance companies have their own security issues. Here is a post in author Mitch Tanenbaum's nationally recognized blog that describes the recent, very embarrassing hack of Lloyds of London: https://cybercecurity-mitch-tanenbaum-blog.com/security-news-for-the-week-ending-october-7-2022/

7.2 Credit Rating Agencies



Credit rating agencies like Moody's Investor Services and Fitch Ratings are now factoring in how companies respond to cyber attacks when calculating credit ratings. These ratings not only affect the creditworthiness of these companies, they will also affect the valuation of them. Credit rating agencies have determined that even if thereare no short-term effects of acyber attack, there very well may be long-term negative effects. How a company responds to an attack says a great deal about the company's leadership and their commitment to protecting the company's assets an

[19] https://www.theregister.com/2022/11/08/government_cyber_insurance/

[20] https://www.wsj.com/articles/credit-raters-look-more-carefully-at-how-companies-respond-to-cyberattacks-11666863002

7.3 Data Protection and Company Valuations

In May of 2019, Raymond Hutchins, one of the authors of this position paper, approached the National Association of Certified Valuators and Analysts (NACVA) with (what seemed to Ray) an obvious question. The NACVA is the organization that sets the standards for how business valuations are conducted. Ray's question was, "Is a company's cybersecurity maturity consideredas a valuation metric in business valuations?" The answer (at the time) was no, but the NACVA asked Ray to write an article about the subject, which then led to the first formal efforts to account for cybersecurity maturity in valuations.

Today, it seems obvious to any business leader that a company committed to protecting the data it is responsible for via professional risk management and cybersecurity practices is worth more thana company that is not. Cybersecurity assessments are now routine parts of the valuation processes used by venture capitalists, private equity firms, banks and other investors. Here is a link to Ray's article: https://www.turnkeycybersecurityandprivacysolutions.com/pdf/ValueExaminer-CybersecandCompan yValuationsSep2019.pdf

7.4 Complying with Cyber and Privacy Breach Notification Laws

If your company or organization suffers a breach, when and who must you report this to? In terms of when you must report, that can be "as soon as you know about it". That can be as short as 24 hours or as long as 30 days. It happens fast, and you must be ready to respond. You cannot figure this out when it is happening.

With respect to whom you must report it to, the answer to that question depends upon:

- The industry you are in.
- The physical location of the breach.
- The location of the owners of the data breached.
- Your compliance requirements.
- The state and country where your company is located.
- The state and country where the "data subjects" (the people whose compromised data) are.
- Vendor and partner contractual obligations.
- Insurance requirements.
- The size and nature of the breach.

And it may include:

- States Attorneys General
- Vendors
- Customers
- Law Enforcement
- Federal Trade Commission
- Insurance carriers
- Industry Regulators
- National security agencies as required
- Your company staff and their families
- Banks

And on and on, depending upon your situation. Again, this information should be readily availablein the company's pre-prepared and tested Incident Response Program.

7.5 Breach Reporting Requirements

As we said, every state currently has some form of law or laws covering these subjects. Likely multiple laws, written at different times, by different people, who will never have to comply with any of them. This reality makes things harder for businesses. Each state has different rules–different rules for what must be reported, to whom and when–different rules for what is considered protected–different rules for how you must handle the information. And some states have very basic laws, while others have more sophisticated ones.

The extraterritoriality requirements of state laws make life very difficult for companies. Let's say that you have a tiny breach of 1,000 records. Because you do not have (or do not enforce) a records retention policy, some of this data is 10 to 20 years old. Of the 1,000 records (people), at the time you collected this data on, may have lived in five states. Since this data is old, it is likely that you don't have a current address for some of them. You are still required to notify them. So, you hire a company to find the current addresses for you. This costs money and time. Same issue with privacy laws. You didn't disclose your plans for the use of the data that you collected, but now the state law for the state these people lived in at the time (but maybe not now) requires that you redisclose your intended use.

You must take those 1,000 records, find these people, figure out where they live now, understand which laws apply, etc. In the case of a breach, you must understand who you are required to notify(such as the state AG, state regulator/s, state police, and national credit reporting agencies, among others). This may depend upon the number of people affected in that jurisdiction.

This must happen before you can use the data for alternate purposes or, in case of a breach, within the breach reporting timeline.

Most notably, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), thus far the most sweeping cybersecurity disclosure mandate applicable to the private sector. CIRCIA requires "covered entities" to disclose substantial cyber incidents to the federal government within 72 hours and ransom payments within 24 hours. CISA is directed to propose rules implementing the
legislation within two years of enactment (i.e., by March 15, 2024); the rules then must be made final within 18 months. CIRCIA's coverage is expected to be broad and could apply to those critical infrastructure sectors identified by DHS, which range from communications and financial services to water systems.

8.0 The Impact of New Technologies

As previously mentioned, AI, quantum computing, IoT, and crypto currencies pose *huge* new risks to the global IT infrastructures and associated financial systems. Again, business leadership will not be capable of reacting fast enough to protect the fragile social fabric–so once again, it will be up to governments to respond.

Here's a glimpse of what is involved:

- **Internet of Things**: Thankfully, there are a lot of efforts globally to bring some kind of order and security to the IoT world. See the footnote below for a link to an authoritative report on the subject. We recommend Bruce Schneider's excellent book *Click Here to Kill Everybody* which presents policy solutions to the critical issue. However, given that there are tens of millions of devices already deployed, retrofitting that inventory will be a major challenge.
- **Quantum Computing and AI**: While quantum computing (and the new threats associated with it) have arrived, there appears to be little appetite for regulating any aspect of it. Governments around the world are funding it to one degree or another, so they have their fingers in the pie, but no real regulation has happened yet.

  Anyone with access to a quantum computer has capabilities that those without access do not. This includes the capability of defeating current cyber defenses.

  Now throw artificial intelligence into the mix. What happens when an authoritarian government has a quantum computer and wants to employ it against us in the cyberwar? China has made it a national goal to be the leader in quantum computing and AI. One of the reasons that adversaries like China are stealing our data now (even data that is encrypted) is that once they have sufficient quantum computing power, they will be able to decrypt the data they stole years before.

  Technologists such as Elon Musk regularly state that AI is a very real threat to humanity's existence and that it must be regulated ASAP. The EU via the European Commission's proposed Artificial Intelligence (AI) Act attempts to regulate a wide range of AI applications, aligning them with EU values and fundamental rights through a risk-based approach. Have you heard about Chat GPT?
  Keep an eye on this.

- **Crypto Currencies**: In this digital age, there are great and growing concerns about the reliability and security of our government-regulated, legacy financial systems and *currencies*–essentially the lifeblood of our civilization. Our financial systems and currencies are only as good as the governments backing them and the security of the IT infrastructures making them function. In very short order, we have digitized the entire financial system. Everyone's money is in digits and those digits are being stolen to fund the adversaries that are attacking us

  As a result, there is urgent interest in a better system and it seems to revolve around crypto currencies. Such currencies are already legal all around the world and many governments are attempting to regulate and/or own them. But in all cases, people access such currencies via software. How do you regulate crypto currencies *and the software* that lets people use such currencies? How do you deal with bugs in this class of software which allows hackers to steal hundreds of millions of dollars with just a click of a mouse–from anywhere on the planet?

  Just one crypto currency platform, Tornado Cash, was used to launder $7B in virtual

currencies[21], including $455 million for the North Koreans alone.
There is great hope (and speculation) that blockchains and the new crypto currencies can evolve our financial systems beyond the control and corruption of humans. The goal is that no matter what happens to the rest of the IT infrastructure, the money will be safe…and that its core value cannot be corrupted by humans or artificial intelligences. However, cryptocurrency is, fundamentally, just software–and software has bugs. Complicated software has a lot of bugs. That is why, for example, crooks have already stolen close to $2billion in cryptocurrency from just one part of the cryptocurrency ecosystem.

9.0 Committed Governance: The Missing Piece–*and the Solution*

Repeatedly, we find that the main obstacle for those who wish to build professional risk management and cybersecurity programs is a lack of commitment by the leadership. In military terms…*if the generals are not fully committed to the battle, there is no way you will get the support of the troops.*

Committed leadership. Committed governance. Without it, the ball does not move down the field.

An example of just how prevalent this problem is within our business hierarchies is that Gartner reports that less than 10% of boards currently have a dedicated cybersecurity committee. That's the bad news. Gartner predicts that 40% will establish one by 2025. That's more bad news, meaning that by 2025 only half of boards will have committed cybersecurity governance.

There are many reasons for the lack of committed leadership and governance.

- Historically, boards and executive management have not been correctly incentivized to tackle the issue. The thinking has been…if it doesn't immediately drop to the bottom line, then it's not worth doing.
- Lack of understanding of how truly secure IT infrastructure is translates into less risk and increased corporate value.
- Unwillingness to buck the internal legacy establishment with respect to raising alarms and providing the funding required for improvements.
- Unwillingness to view cyber risk with the same degree of alarm that legislators and regulators do.

But this is changing because of many factors:

- New government regulations (like the FTC and SEC changes)
- Customer demands (we are not going to do business with you unless you …)
- Insurance company demands (we are going to cancel your insurance unless you …)
- The Caremark Standard
- New state laws
- The change in federal courts' views on what constitutes Article III Standing, making lawsuitseasier

Achieving Committed Governance Requires the Following:

A successful cybersecurity and privacy program requires fully committed leadership and hands-on governance. And once leadership commits to the battle, its on-going support must never waiver. Itbecomes part of the business operations. The commitment includes:

- A company Risk Management Program that highlights cybersecurity and privacy.
- An acknowledgement by the board and executive management that cybersecurity

and privacy negligence may threaten the existence of the organization and can result in *personal liability for leadership.*

- Written risk governance procedures for the board and executive management.
- Designated individuals on the board and within management whose compensation is tied to specific cybersecurity and privacy metrics.
- Recalculation of the organization's financial valuation that accounts for organizational risk associated with cybersecurity and privacy.

With the stakes so high, directors and leaders must do the following:

- Continue to elevate the importance of managing cybersecurity risk on a company-wide basis, and not just as an IT matter.
- Ensure proper disclosure. Enhanced disclosures clarify for investors and other stakeholders the rigor of the board's oversight, and management's role in assessing and managing cybersecurity risks.
- Break out of their silos and echo chambers and promote a culture of cooperation, both internally and with other organizations.
- Utilize outside parties to help expand knowledge bases, strengthen capabilities, and identify blind spots in security and risk management.

[21] https://www.nytimes.com/2022/08/08/technology/treasury-blacklist-crypto-tornado-cash-laundering.html

10. How We at Turnkey Cybersecurity & Privacy Solutions Can Help

Clearly, this is a challenging problem for SMBs. It's not something that can be solved in a week. It's not something you can solve by yourself. If you are ready…if you have the commitment, then we can be the partner you need.

Together we can diligently build a risk management program that will reduce risk, protect your assets, and increase your company valuation. And using our proven systems and processes, wecan do this for minimum expense and brain damage.

Please call or email us to learn more:

Raymond
Hutchins Mitch
Tanenbaum
Partners
Turnkey Cybersecurity & Privacy Solutions,
LLCCyberCecurity, LLC
303-887-5864
rh@cybercecurity.com
mitch@cybercecurity.com

Did you find this position paper of value? Here are some of our other papers.

- IT Infrastructure Monitoring Issues-Making the Best Choice for Your Company
- Secrets of Hiring and Firing vCISOs
- CMMC Compliance-The New Enclave Approach
- The "NEW" CMMC 2.0 (AKA 800-171): Not the Right Way to Fix the DIB Security Crisis

About the Authors

Ray Hutchins and Mitch Tanenbaum own and operate two cybersecurity companies:

- CyberCecurity, LLC
- Turnkey Cybersecurity and Privacy Solutions, LLC

These are veteran-owned, mission-oriented companies providing defensive governance, strategic and operational guidance, and boots-on-the-ground support to organizations that acknowledge the cyberwar and are ready to actively support and engage in risk reduction and value creation.

Ray's and Mitch's wide range of cyberwar experiences with defending organizations all over the world and their ability to articulate this complex technical environment to leaders has established them as "global cyberwar" authorities. Please learn more about Ray and Mitch here: https://www.cybercecurity.com/about/