HEALTH - ISAC
NAVIGATOR™
PROGRAM

2021 ANNUAL REPORT

THE STATE OF HEALTHCARE SECURITY & PRIVACY

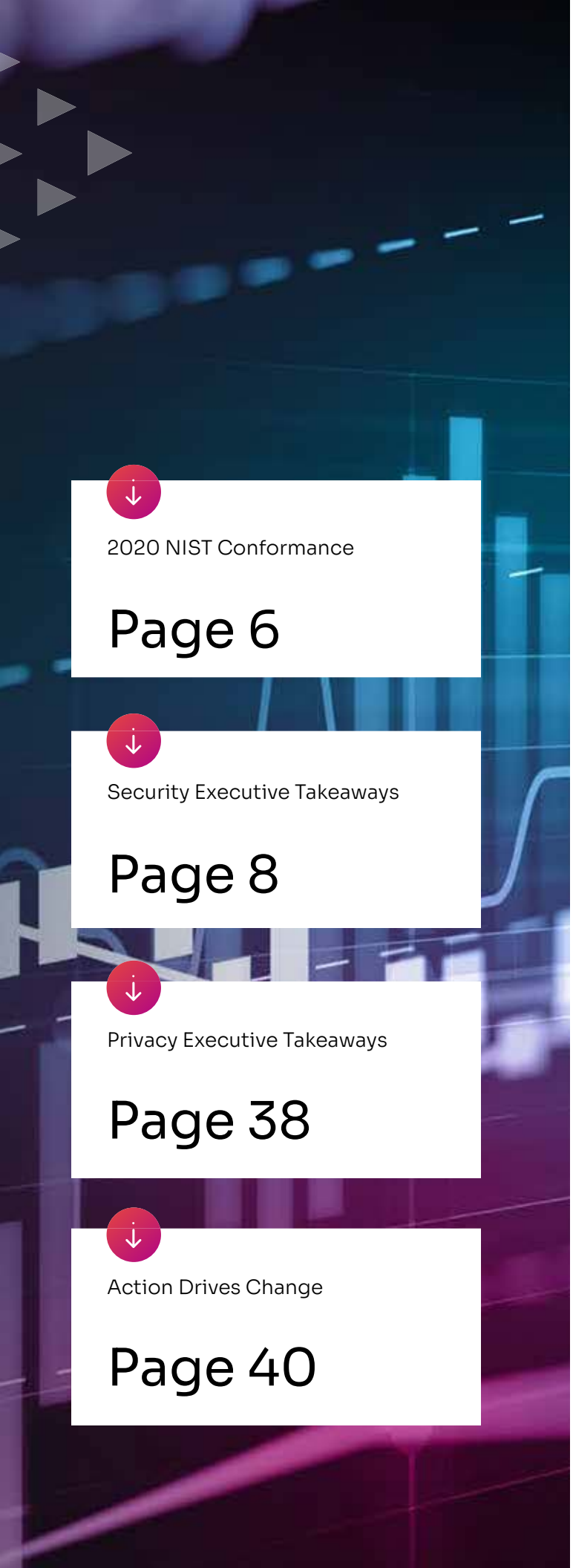
Maturity Paradox:
New World, New Threats, New Focus

CynergisTek

2021

ANNUAL REPORT

I.	About CynergisTek	3
II.	Disruption Leads to Change	4
III.	2020 NIST Conformance	6
IV.	Security Executive Takeaways	8
V.	NIST Conformance by Function	10
VI.	Data Privacy in 2020	30
VII.	Privacy Executive Takeaways	38
VIII.	Action Drives Change	40



2020 NIST Conformance

Page 6

Security Executive Takeaways

Page 8

Privacy Executive Takeaways

Page 38

Action Drives Change

Page 40

ABOUT CYNERGISTEK

CynergisTek is a team of cybersecurity, privacy, and compliance problem solvers and experts dedicated to helping healthcare organizations prepare, rehearse, and validate the effectiveness of their programs. CynergisTek's Resilience Validation™ method takes a unique coach-to-client partnership to ensure you achieve your goals, build cyber resilience, and have an approach that responds every day. CynergisTek offers comprehensive service solutions categorized under the four pillars of Assess, Build, Manage, and Validate.

DISRUPTION
LEADS TO CHANGE

Care Delivery

As CynergisTek delivers our 2021 annual report, it goes without saying that COVID-19 impacted virtually every organization and person across the globe over the past year – a peerlessly devastating pandemic that simultaneously reshaped industries, including ours. The world was forced to accelerate digital transformations that might otherwise have taken years, creating new cybersecurity challenges, particularly within the healthcare sector.

While providers focused on caring for patients during the pandemic, they also had to embrace new care and IT delivery models. Countless workers became remote, switching to devices that ranged from personal to corporate, managed or unmanaged, and sometimes shared with multiple users.

Faced with change, clinicians, administrators, and boards rapidly embraced IT as a strategically important component of care, even if security and privacy remained afterthoughts. At the same time, the 21st Century Cures Act introduced new electronic health record information and interoperability mandates designed to promote data sharing, notably without technical security requirements for APIs. To the extent that 2020 dramatically impacted the healthcare sector's data and IT practices, it's clear that those changes are only continuing – and increasing – in 2021, a trend that will continue for years to come.

Data Privacy has become a top area of responsibility for security professionals, with

34%

of survey respondents indicating privacy is one of their core competencies and responsibilities.

Source: Cisco 2021 Data Privacy Benchmark Study Forged by the Pandemic: the Age of Privacy, January 2021

Ransomware attacks cost the healthcare industry

$20.8 billion

in downtime in 2020, double the number from 2019.

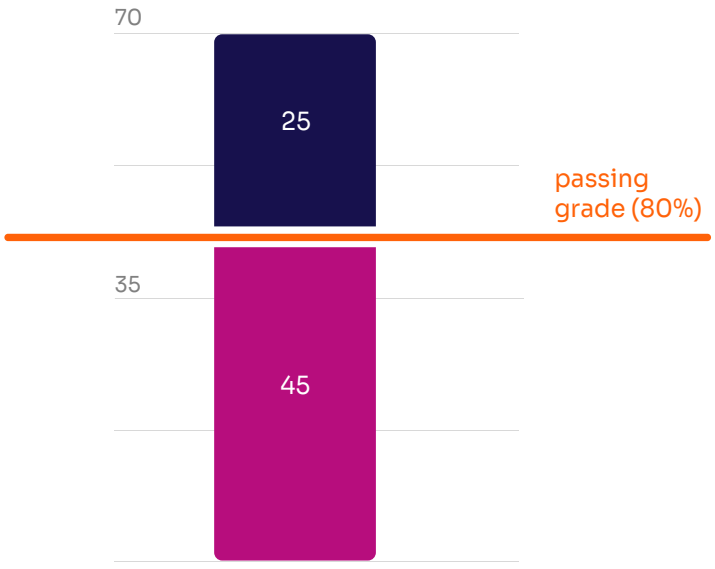
Source: Comparitech Annual Report

IT Delivery

This year's report focuses on how well the healthcare industry is progressing instead of simply reporting "scores" and conformance with The National Institute of Standards and Cybersecurity Framework (NIST CSF) and the HIPAA Security Rule. Today and in the future, it has become critical to actively work to reduce cyber risk to the business on a continuous basis - - as the business, technology, regulations and rules, and threats and attacks change. In 2020 we saw record ransomware attacks on healthcare, attacks that used our vendors and third party suppliers and that it's continuing into 2021. Yet, still, over half of the sector (64%) is below what we would consider a passing score. Security will always be a journey, there is no stopping - - until technology stops advancing, until healthcare stops using technology, until bad guys decide to leave healthcare alone. There is no stopping on the security journey.

Security is a journey therefore we focused this year's analysis on how the industry is improving overall, focusing on two cohorts from the 2020 data: high performers with a conformance score **over 80%**, and the remainder as low performers.

State of healthcare security



64%
of the organizations are below the passing grade

In 2020, 560 healthcare provider facilities fell victim to ransomware.

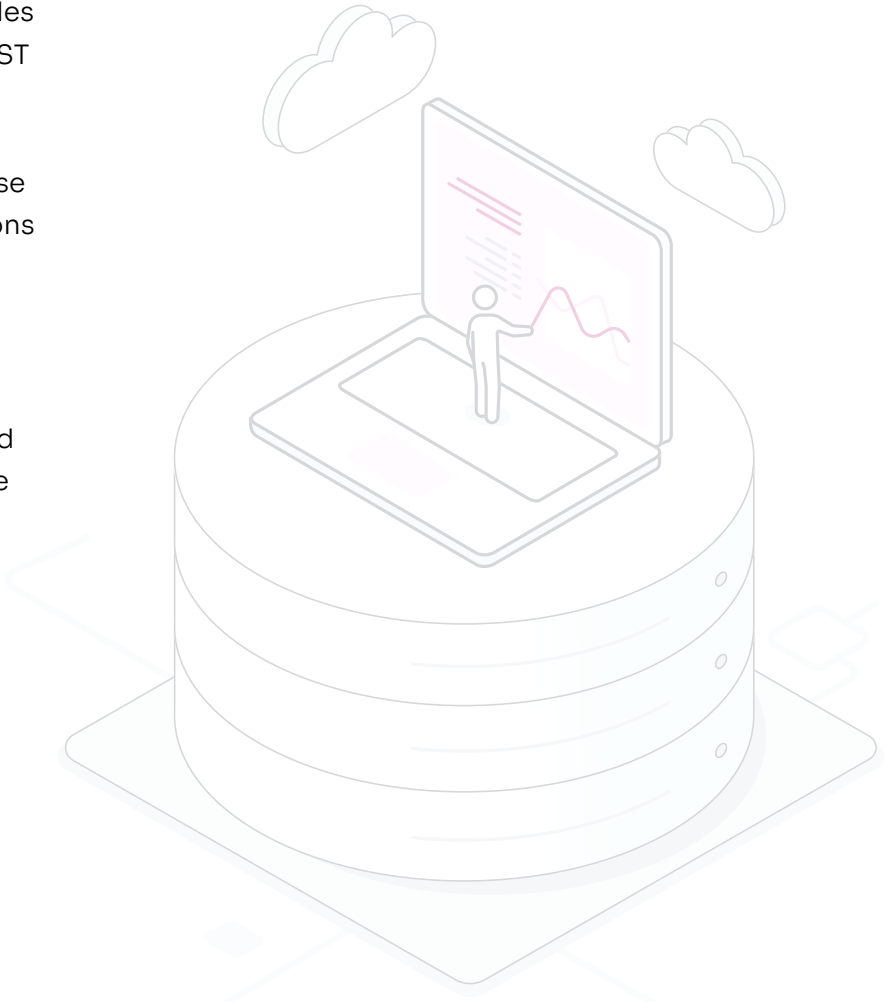
Source: Emsisoft State of Ransomware Report

2020
NIST CONFORMANCE

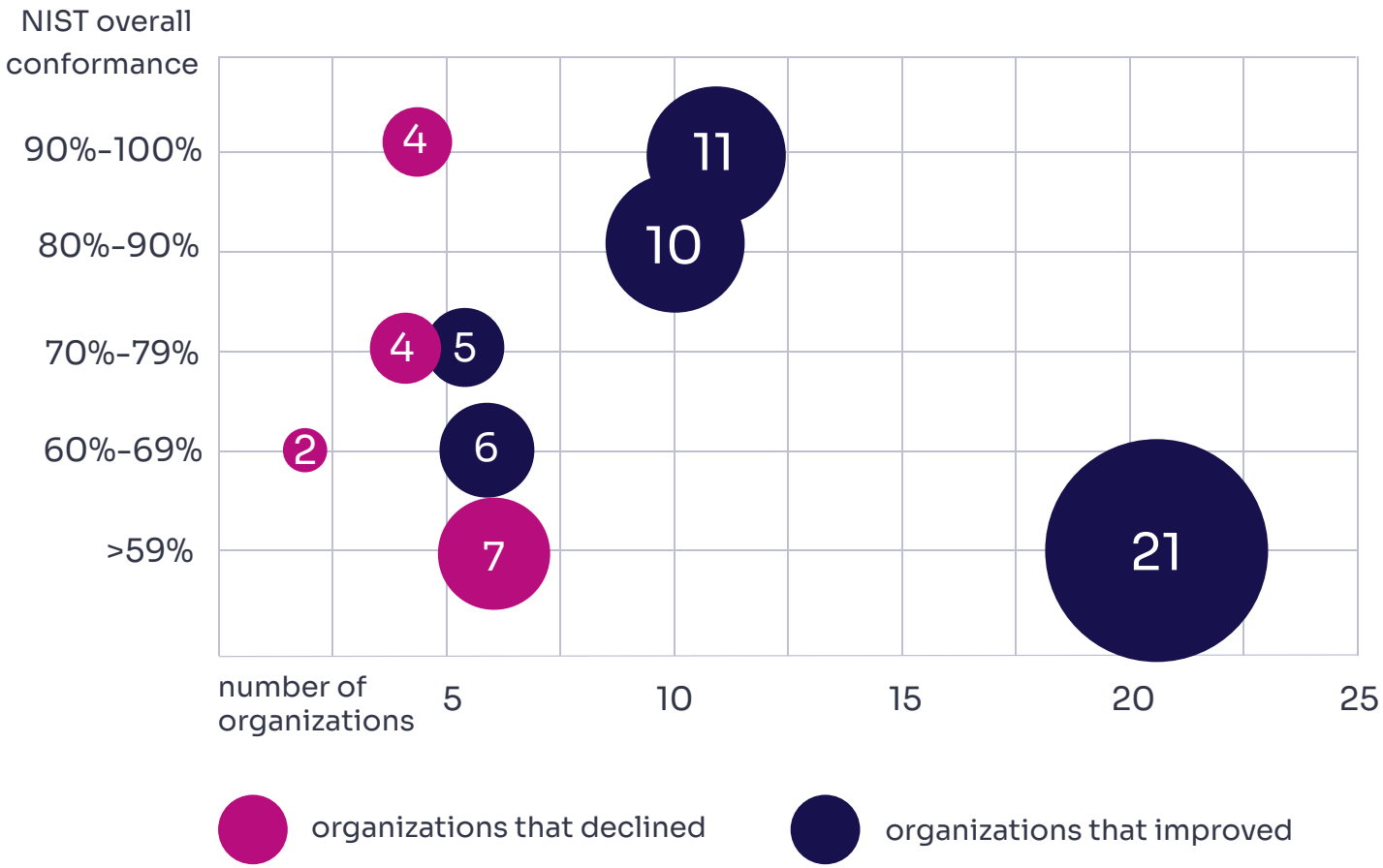
In 2020, the COVID-19 pandemic led to a delay in annual risk assessments leading to a smaller sample size of 100 assessments compared to data from previous years.

Measuring progress alongside overall NIST conformance provides a complete picture of the healthcare industry's current state of security. In this graph, we analyze organizations that have improved or declined by their NIST overall conformance. Even though 75% of the industry improved during COVID-19, most of these strides are small and are far from the accepted 80% NIST conformance.

With the bad guys continuously changing course and innovating, it is imperative that organizations must invest in improving their security posture to stay one step ahead of these bad guys. If organizations chose to do nothing, NIST CSF scores will not only decline but will put the organization at greater risk for cyberattacks and less resilient than those organizations that have invested in security and privacy.



Improve or Decline: YOY Performance



SECURITY
EXECUTIVE TAKEAWAYS

Last year, we noted that "the industry may be too focused on getting good grades rather than reducing risk," and that while comparisons are useful to provide big picture awareness, "they do not reduce your risk or protect you. This is not about the scores." We decided to take our own advice this year, so rather than diving into year-over-year trends or NIST and HIPAA conformance, we are not focusing on scores.

Instead, we wanted to see what organizations are doing, the core functions of NIST that seemed to drive long-term improvements, and what will drive the direction for Health IT Security over the next twelve months, as threats and attacks grow worse and more numerous. Our intent is to identify opportunities for short- and long-term success.

The three key industry trends we are seeing are:

1 An ever-expanding cyberattack surface.

Healthcare is facing new and augmented challenges from multiple directions, including an increasingly mobile and remote workforce, telehealth, telemedicine, IoT, consumer medicine (as impacted by the 21st Century Cures Act), and concerningly, the supply chain.

2 Ransomware is a cyber weapon of choice.

COVID-19 inspired hackers to pursue ransoms as companies rushed to digitize without adequate security measures, creating more extortion targets. While Help Net Security reported a 358% year-over-year increase in malware overall, research from Deep Instinct found that ransomware specifically increased by 435% from 2019 to 2020, and Coveware reports that the average ransomware payout has grown to nearly $234,000 per event.

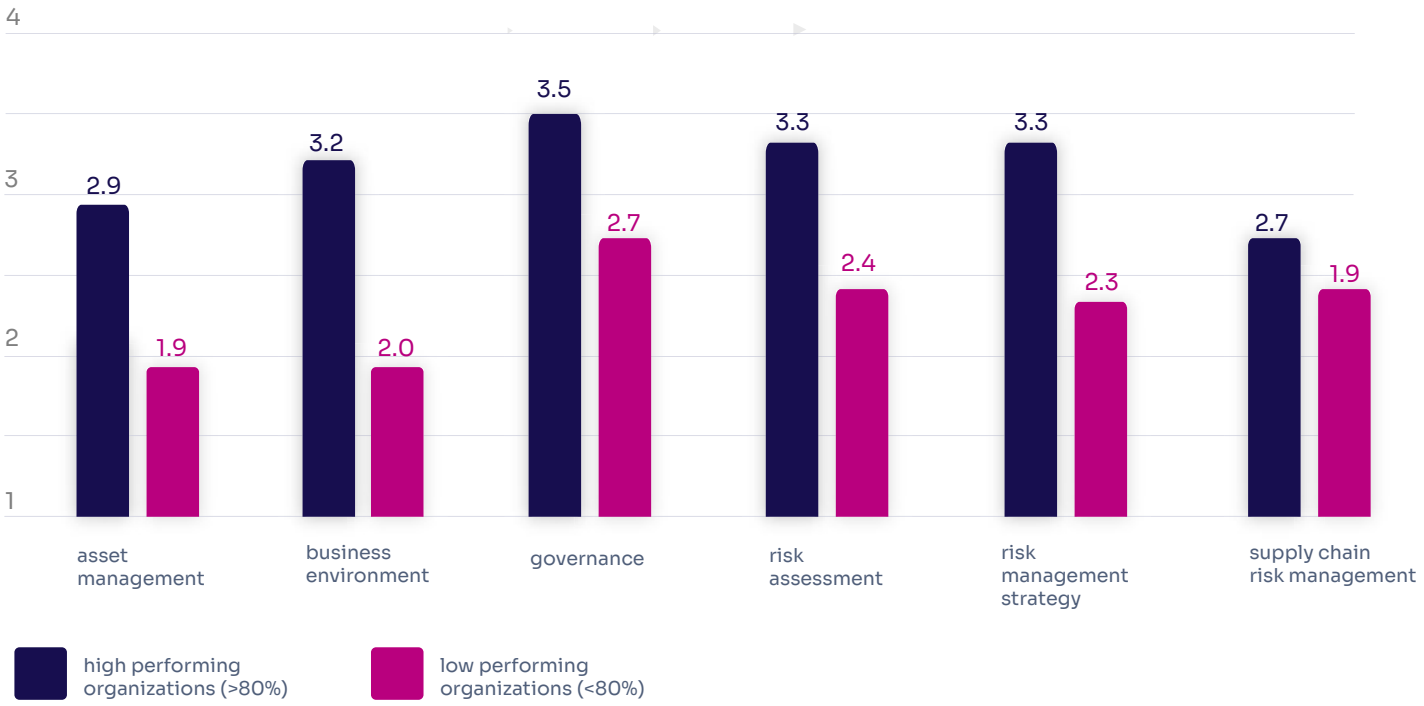
3 Threats against critical infrastructure.

Healthcare is one of the U.S. government's 16 critical infrastructure sectors. Threats have recently spread past computers to include Industrial Control Systems (ICS) -- everything from freezer sensors to badge readers -- and converged Operational Technology/ Information Technology (OT/IT) networks, notably including medical devices.

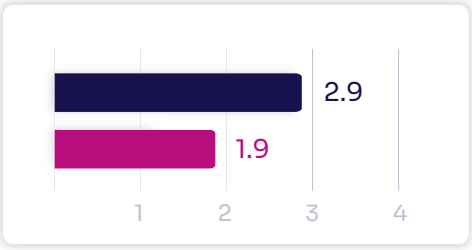
NIST CONFORMANCE
BY FUNCTION

Identify

The Identify function is the first of the five Framework functions. As such, it provides the foundation for the rest of the functions to be built upon. This function centers around pinpointing all organizational systems and platforms, including data, included in its infrastructure.

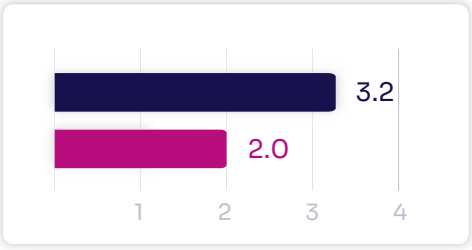


Asset Management



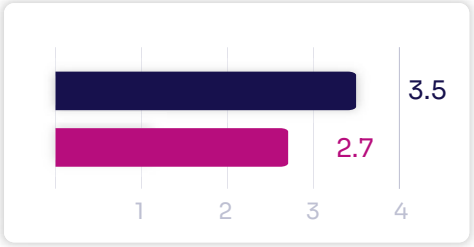
With 73% of this sector falling into low performers is not a good starting point and Asset Management should be a key focus area to reduce risk by prioritizing and classifying your resources, evaluating all assets including the **data that flows through the devices** including medical devices, and lastly ensuring roles and responsibilities are established not just written down on paper.

Business Environment



Low scores in Business Environment indicate that security is not clear of their organization's role in the critical infrastructure, **discussions at the C-Suite and Board-level are not happening**, and resilience requirements to support delivery of critical services is concerning given the recent ransomware attacks on healthcare while dealing with a global pandemic.

Governance



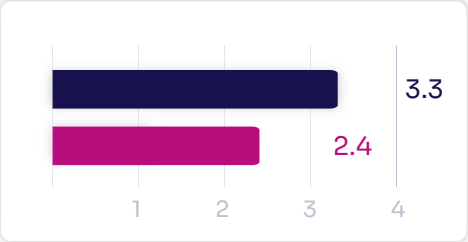
Overall, the Governance category is either on its way or is well established however where did find three key areas that need to be addressed

1. Identifying and knowing who does what in terms of security at the organizational, departmental, personnel level internally and externally.

2. Understanding the **legal and regulatory requirements to support and update policies and procedures.**

3. Implement risk management processes designed to address cyber risk.

Risk Analysis



In the Risk Analysis category, the High Performers truly stand out against the Low Performers with over 90% conformance across the board. **You cannot protect what you have not identified, nor can you track the controls and mitigations you have implemented.** Areas for Low Performers to focus their efforts need to be in the following areas:

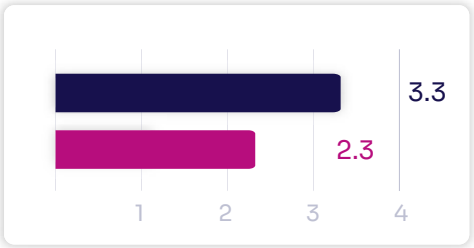
1. Collecting and sharing threat intel, identifying documenting both internal and external threats.

2. Identifying and understanding the impacts and likelihoods of a cyber event occurring is the heart of risk management.

3. Once threats & vulnerabilities are identified we, as a sector, have not moved to using likelihoods and impacts to determine risk.

4. Not prioritizing risks and responses may well indicate that resources are being applied to lower risk issues and, worse, high-risk issues are not getting timely and appropriate attention.

Risk Management Strategy



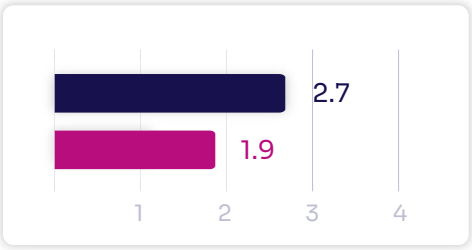
The Risk Management category ties in closely with the earlier Risk Analysis category. **If organizations are unable to identify risk, then it will be difficult to determine your risk tolerance.** The healthcare industry will continue to lag in this category if the previous areas including the lack of understanding of the organization's role in critical infrastructure, threat intelligence, clear risk analysis, and risk tolerance are not made a priority.

Cybersecurity is about sharing, about transparency, and we are all part of a much bigger cyber world than our own because we connect and share so much with so many organizations and individuals.

high performing organizations (>80%)

low performing organizations (<80%)

Supply Chain Risk Management



Supply chain overall was the lowest category across the board. Supply Chain is clearly a latecomer even among organizations that have significant improvement over a 4-year period. CynergisTek started assessing against NIST CSF 1.1 in 2017 but some organizations delayed adoption because they were in a cycle on their POAM (Plan of Action and Milestones). It will be interesting to see the curve in this category over the next few years.

Both the High Performers (50%) and Low Performers (30%) have **low conformance with taking the appropriate measures to help the organization meet the security and risk management plan** objectives of contracts with third parties and suppliers. In addition, organizations lack routinely assessing or other forms of evaluations to confirm third parties and suppliers are meeting the obligations that should have been set form in the contract.

Most notably, given the events of 2019 and 2020 with the attacks on critical third parties and suppliers, from Solar Winds to the Colonial Pipeline, it is clear that response and **recover planning and testing scored low** and is a critical area to focus on going forward.

Supply Chain was the second lowest-scoring and least mature category across the board with an average score of

2.7

The main issue was the failure to confirm that third parties are meeting contractual security obligations.

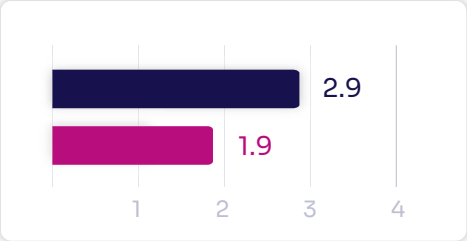
Protect

The Protect function is essential because its purpose is to develop and implement appropriate safeguards to ensure critical infrastructure services delivery. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

56%
of healthcare organizations believe a cyber attack will occur as a result of a medical device, and only
15%
of organizations are taking the necessary steps to prevent it.

Source: Ponemon Institute Survey

Access Control



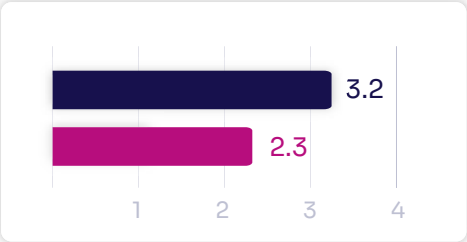
Identity Management, Authentication and Access Control (AC) under the Protect Core Function (PR) performed just above the low performing category Identify: Supply Chain.

Starting with identities and credentials being issued, managed, verified, revoked, and audited for devices, users, and processes. The High Performers could not get to a 3 again, coming in at 2.9. Unfortunately, the Low Performers, 73% of our assessments did not even get to a 2 - - coming in at 1.9. In terms of managing remote access (PR. AC-3), we suspect we have found an issue with timing given the events of 2020 and remote work and remote care. High Performers are still sub-3 and Low Performers could not get to a 2 (1.9). **Given the types of attacks often existing accounts with elevated privileges coupled with the amount and types of remote access, protecting identities, credentials for users, and devices and processes need to be stepped up across the sector.**

Network segmentation and micro-segmentation is not only a management tool for isolation in the event of an attack but it can also be used in offensive protection around medical devices, for example, in terms of mitigation of medical device security issues by way of leveraging your network topology - - which devices talk to which other devices on and off your network, what they are "saying" and when they may talk. Least surprising in this sub-category related to the protection of network integrity focused on network segregation and segmentation is the low point. Network segmentation and micro-segmentation is not only a powerful tool in the event of attack through isolation, but it can be used to proactively defend non-compute devices and IoT (Internet of Things). Medical devices that may not be able to be patched or updated may be protected by leveraging the network's topology. **Network segmentation should be on every organization's road map, it is not already completed.**

Since the sector does not do a decent job of evaluating or determining risk or risk tolerance, it will be interesting to how it responds to new attacks in terms of authenticating users, devices, and other assets - - let us just say that multi-factor is better, in most cases - - commensurate with the risk of the access and/or transaction.

Awareness and Training



Awareness and Training should be the easiest and least costly category to address. Please note, I said should, the data does not appear to support this proposition, however. People are your first and last line of defense. **This Category under Protect (PR) is clearly neglected.** We see it daily in the number of successful attacks of all kinds against the sector.

The bulk of our assessments attained 50% - - think about the fact that only 50% of the sector is training and informing users on an ongoing basis about security. Many have not even gotten to the one-half level. Same song, different verse with privileged users understanding their roles and responsibilities. The theme continues with 3rd party stakeholders and assuring they understand their roles and responsibilities through initial training and ongoing awareness.

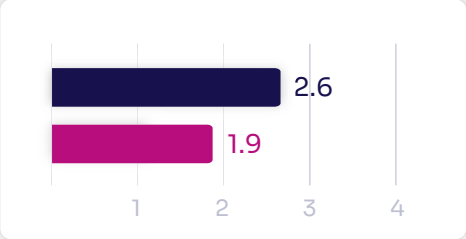
One of the worst sub-categories is Awareness and Training and, frankly, a critical one. Senior executives (including the Board) understand their roles and responsibilities. Enough said. Except that IT (Information Technology) and Security is not about IT and Security - - it should be about patient care and clinical and business operations. The Board has ultimate responsibility for funding and providing strategic goals, guidance, and authorizing funding. That is not IT and Security. **Senior executives and the Board have special obligations and fiduciary responsivities. Train and educate them.**

high performing organizations (>80%)

low performing organizations (<80%)

In Data Security, the High Performers met a 90% conformance for **Data-at-Rest** (PR-DS-1) while the rest of the sector was in the low **30th percentile.**

Data Security



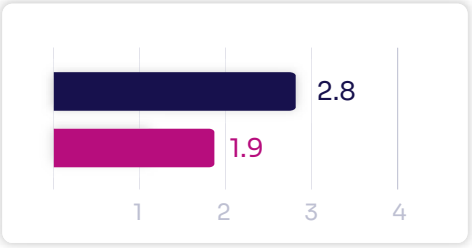
As we move into Data Security (data at rest and in transit), some interesting and disturbing anomalies begin to emerge. Encryption, in the early days of HIPAA, (Health Insurance Portability and Accountability) was hailed as a "get out of jail free card" in terms of breach notification. **An organization's default for storing protected data of any kind and transmitting it should include encryption - - it clearly does not.**

On a happier note, most organizations have fully implemented controls to assure there is adequate capacity to ensure availability to data is maintained.

The sector lags in fully implementing Data Loss Prevention (DLP). DLP is not simply a tool. DLP is an enterprise program. It is ongoing and since the data you are preventing the loss of is used by many, many departments it is no more an IT project than is putting in an EMR. It is not surprising that this sector has struggled with implementing enterprise-wide DLP. It is not uncommon to see it in use on specific data elements or systems (email).

Maintaining development and testing environments that are separate from production is considered a best practice in all sectors. A best practice in which healthcare lags. A more arcane sub-category but one that will also likely grow in importance is integrity checking to verify hardware integrity. During 2020 we found that the High performers hit 80% across the sector of "largely" or "fully" implemented.

Information Protection Processes and Procedures



Overall, the sub-category creating and maintaining baseline configurations of IT and Internal Control (IC) systems that incorporate core security principles (e.g., least functionality) should be a focus area across the sector.

A System Development Life Cycle (SDLC) to manage systems is basic IT operations. We were surprised to see the overall low implementation level here. Change control is also a core function of IT operations. Outside of the top of the High Performers there is little in formal and functional SDLC.

Repeated warnings around best practices for ransomware attacks always include backups of information – – they are conducted, maintained, and tested. Considering those warnings and the uptick in ransomware and in healthcare specifically, this may be telling in terms of why so much ransom is paid. As a sector, we do better at protecting the physical operating environment for organizational assets than we do with data.

high performing organizations (>80%)

low performing organizations (<80%)

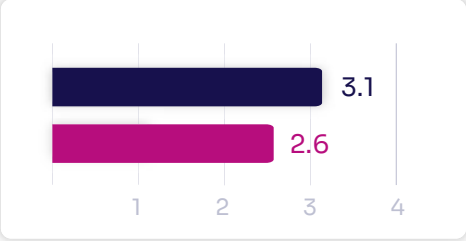
One of the foundational requirements of any security framework, but certainly NIST CSF, is continuous improvement using closed-loop systems and regular feedback and incorporation of changes or new data, capabilities. There is room for improvement. Looking at what you are not doing or not doing well and building those fixes or corrections into newly updated plans, regularly is continuous improvement.

No surprises here. Response and recovery plans are not tested in terms of Information Protection Processes and Procedures. Only the top High Performers were substantially implemented. It dropped off sharply after that.

Echoing back to Awareness and Training we do not see that cybersecurity is included in HR (Human Resources) practices (de-provisioning, personnel screening, etc.).

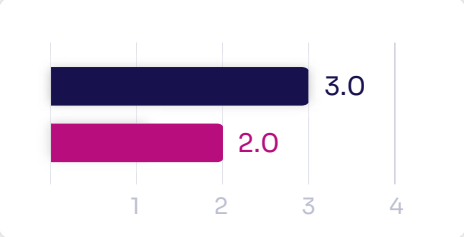
Even though Microsoft's "Patch Tuesday" started in October of 2003, we still see that having a developed and implemented vulnerability management plan is a concern for the entire sector. **This may not mean that organizations are not correcting or controlling vulnerabilities but without a formal plan, followed regularly and timely, it creates opportunities for vulnerabilities to escape detection and mitigation.** In worst-case scenarios these known vulnerabilities may be perpetuated across the organization and even to other organizations that have any kind of data, communications sharing with those failing to manage vulnerabilities.

Maintenance



On an upbeat note, maintenance and repair of organizational assets are performed and logged with approved and controlled tools which is what PR.MA-1 measures. Remote maintenance, however, is not at the same level.

Protective Technology



While High Performers got to a 3.0 in the category - - they did it the hard way. Audit/log records and if they are defined, documented, collected, and reviewed in accordance with policy is a critical function of cybersecurity, it is not, however, a glamorous function. Consequently, we were not surprised to see a comprehensive lack around this sub-category.

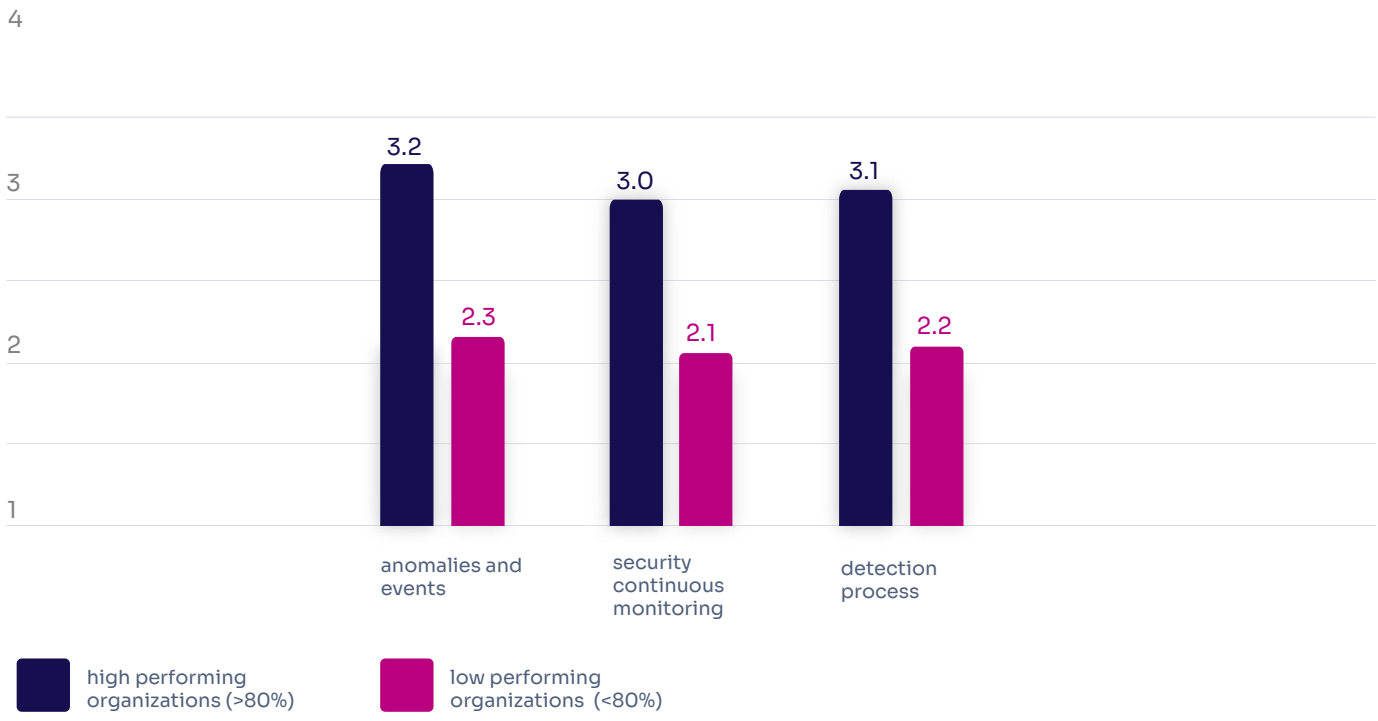
Removable media protections and restrictions, which should be documented in policy were implemented feebly across all assessments.

One high point is that the protection of communications and control networks looks is also a “win”.

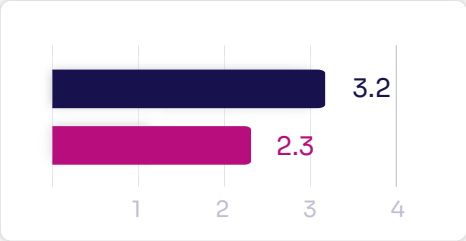
Part of Protective Technology is about the mechanisms to increase resiliency in normal and adverse situations. Given the threat environment, anything less than substantial implementation could spell disaster in the event of a major attack or system failure.

Detect

Moving into the Detect Function, we have seen not only significant levels of implementation across all of our assessments but this an area where High Performers are at consistently elevated levels of substantial implementation with the single sub-category exception of detection of malicious code. This is as much a reflection of the rapidly changing threat environment and the ability of current technologies to detect malicious code as it is about the implementation of best practices.



Anomalies and Events



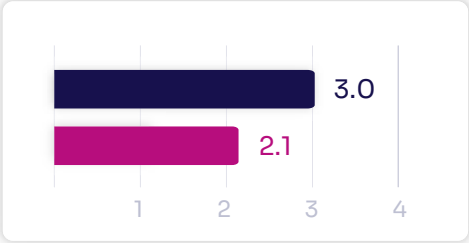
Across the entire sub-category of Anomalies and Events under the Detect Function, the High Performers were all "substantially implemented" with an average of 3.2 across the sub-category. This function is where the organization defines important detection roles, responsibilities, and processes and where they are conscientiously implemented within the organization. **The message here is clear: if you want to be a High Performer, get your Detect Function substantially implemented.**

Data collection and correlation from multiple sources/sensors will need some improvement across all organizations. **Also needing improvement: analysis of detected events to understand attacks and methods.**

Determination of the impact of events seems like it should be straightforward, but it is not being assessed or documented outside of High Performers. **Without a documented impact of events, organizations may be focusing on minimal impact events and not focused on the bigger risks.** This kind of documentation can also assist in reporting cybersecurity effectiveness as well as needs to senior leadership and Boards.

Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Continuous monitoring was one of the early drivers underlying NIST CSF, it is also core to the HIPAA (Health Insurance Portability and Accountability) Security Rule's concept of "ongoing risk management" - - which is the goal of regular risk assessments. **From a technical perspective, however, there are too many things happening too quickly to rely on human observation and intervention thus continuous monitoring of security processes will need to become more automated.**

Security Continuous Monitoring



As previously stated the healthcare industry lags in network architecture (lack of segmentation, micro-segmentation) and we also see this in network monitoring for potential cyber events. As a sector, we fare better at monitoring the physical environment for cyber events.

User behavior analytics will grow increasingly critical with work-from-home and remote care, but we do not watch our people as closely as our own physical environment.

The area of malicious code detection is the lowest scoring area for even High Performers in the Detect Function.

Use of unauthorized Mobile code/systems has been an area that is often knowingly neglected in healthcare or regularly deferred due to higher priority issues. **Mobile will become more prevalent, this is an underperforming area across the sector and will need to be addressed.**

Related to Supply Chain, where all industries and sectors lag is DE.CM-6 monitoring of external service providers for potential security events. This is one area where the effort of the High Performers may help the other cohorts, assuming any findings are shared by the external service provider when events are detected and particularly sharing across the sector when a High Performer detects an actual cyber event at one of these providers.

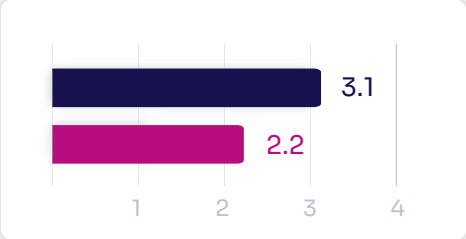
Given the spoofing and elevating of credentials as well as more remote devices from more locations and the use of personal software on managed devices; **monitoring for unauthorized personnel, connections, devices, and software will need to be an area of some focus moving forward.**

Detect, DE.CM-8, requires that vulnerability scans be **performed - - not just planned. Again, given the growing number of devices on the network and the growing number of vulnerabilities being reported particularly around medical devices, this is not a bright spot.** Even High Performers only achieved an average of 3.0.

high performing organizations (>80%)

low performing organizations (<80%)

Detection Processes



Detection does not count if no one knows who is doing it, who they should report it to, and who is accountable for what actions related to detecting potential cyber events. Again, in terms of the Detection Processes category, High performers are at 100% substantial implementation across all sub-categories. Across High and Low Performers, however, the industry average is 2.4.

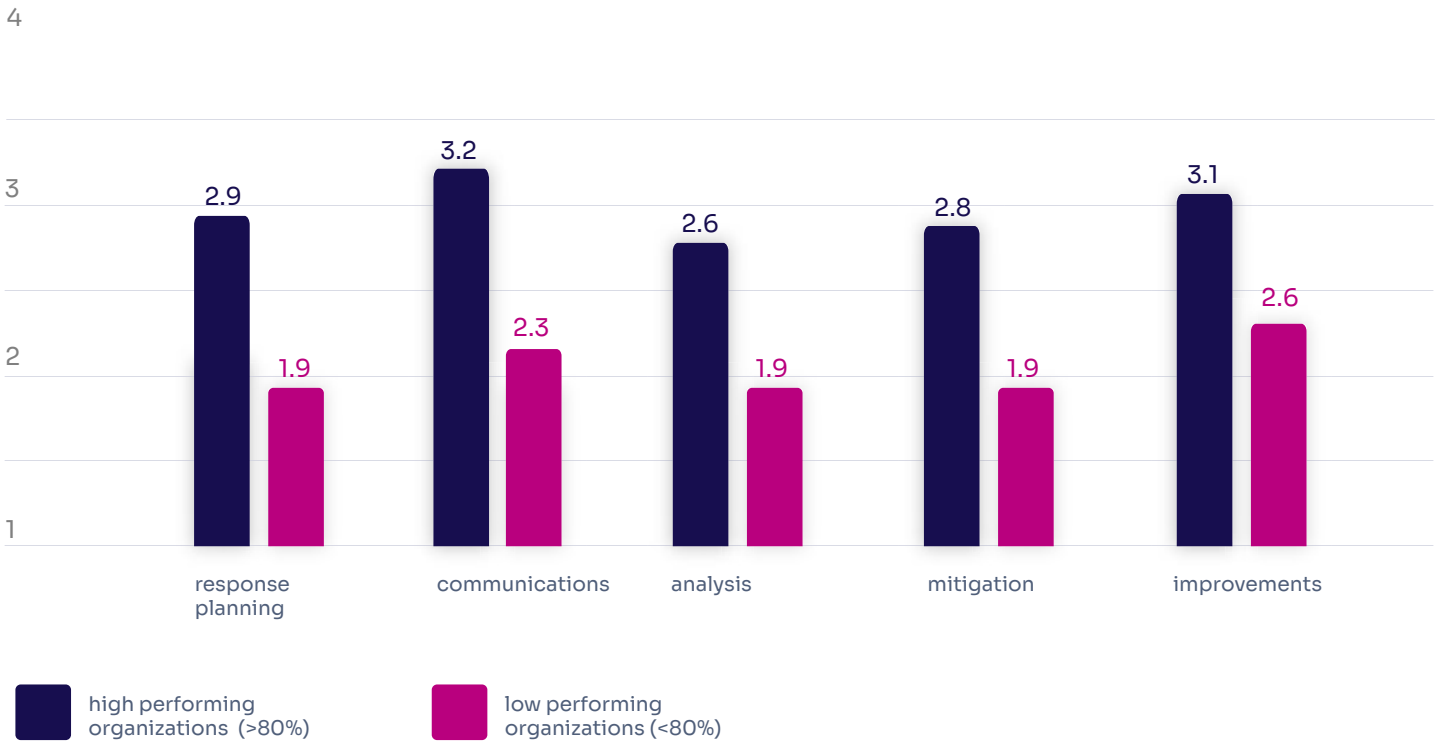
We find that detection processes themselves are not often tested. **This is validating that the controls you have implemented are alerting on the identified events, that the right people are being notified and that the processes delineated in the controls are working as intended.** Detection processes that are not working are no longer detection processes. The failure of these detection processes may make things worse. If you do not have tools, you do not expect messages/warnings from them. **If you have installed them but do not get anything or the alerts go to the wrong place you are working under a false sense of security.**

We do seem to be able to do an adequate job of communicating events when we do detect them.

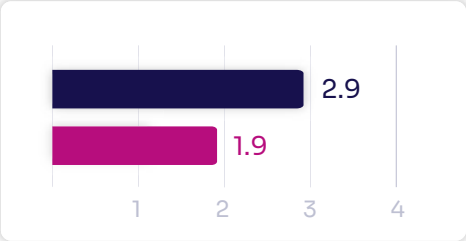
One of the fundamental intents of implementing a security program is continuous improvement. What is the point of doing all this monitoring, alerting, and analysis if we are not using it to get better? High Performers are doing alright, all others will require focus.

Respond

Cyber resilience is the ability of an organization to prepare and respond when cyberattacks happen. An organization has cyber resilience if it can defend itself against these attacks, limit the effects of a security incident, and guarantee the continuity of its operation during and after the attacks. Organizations today are beginning to complement their cybersecurity strategies with cyber resilience. While cybersecurity's main aim is to protect information technology and systems, cyber resilience focuses more on making sure the business is delivered. Its intended outcome is business delivery, keeping business goals intact rather than the IT (Information Technology) systems. The Respond Function is where the organization demonstrates and maintains the development and implementation of appropriate activities to act regarding a detected cybersecurity event.



Response Planning



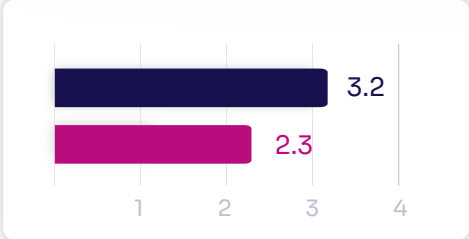
Having a response plan allows you to proactively intervene and prevent or reduce issues that may occur in the event of a cyber incident. An incident response (IR) plan is something that every organization should have in place. It only works if you execute on it during or after an event and unfortunately, that is not what we found.

77%

of companies don't have a consistent cybersecurity response plan.

Source: IBM Security Report, 2018

Communications



An IR plan is only as effective as the people and departments that have a role are prepared to execute on the plan. This is a marked improvement over executing a response.

The sector also appears to do well at reporting incidents consistent with the defined criteria, does share information consistent with the response plans and coordinates the sharing of information with stakeholders consistent with the plan. In addition, our analysis shows that overall sharing of information with external stakeholders with the intent of expanding cybersecurity situational awareness was overall okay among High Performers but needs work in Lower Performing organizations.

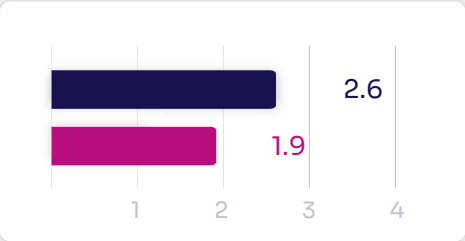
Incident response preparedness can save companies an average of

$2M

during a data breach

Source: IBM Ponemon Cost of a Data breach Study, 2020

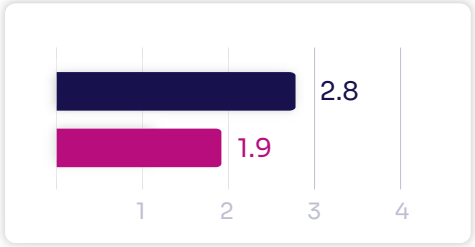
Analysis



Only the top of the High Performing group is actively investigating notifications from detection systems. Fortunately, impacts of an incident are well understood across the sector. While there is room for improvement, the sector is effective at categorizing incidents consistent with response plans. The sector is not as effective as it needs to be at using shared information from both internal and external sources. The sector needs to improve in this area, although we have seen some growth over the past few years.

This category speaks to the heart of the Respond Function - - Mitigation. That is to assure that activities are performed to prevent the expansion of an event, mitigate its effects, and resolve the incident.

Mitigation



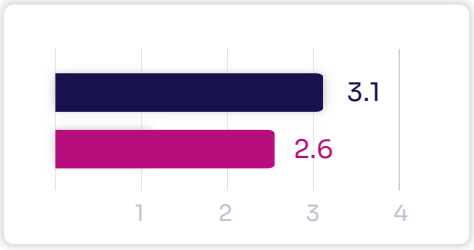
This category speaks to the heart of the Respond Function - - Mitigation. That is to assure that activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

In terms of containing an incident through the response, only the top of the High Performers are doing this consistently and substantially. In terms of being able to mitigate an incident through the response, this is the most troublesome, all organizations are less effective at mitigation than containment. The sector needs to also improve its ability to mitigate and document new vulnerabilities as an acceptable risk.

high performing organizations (>80%)

low performing organizations (<80%)

Improvements



We have already mentioned that the **point of all this effort is to keep getting better** . . . continuous improvement using closed-loop systems and regular feedback and incorporation of changes or new data and capabilities. This category is improvement - - response activities are improved by incorporating lessons learned from current and previous detection/response activities.

If you are not changing and/or updating the response strategies after an incident or even an exercise you are missing the best opportunity to improve. There is room for improvement, based on our assessments.

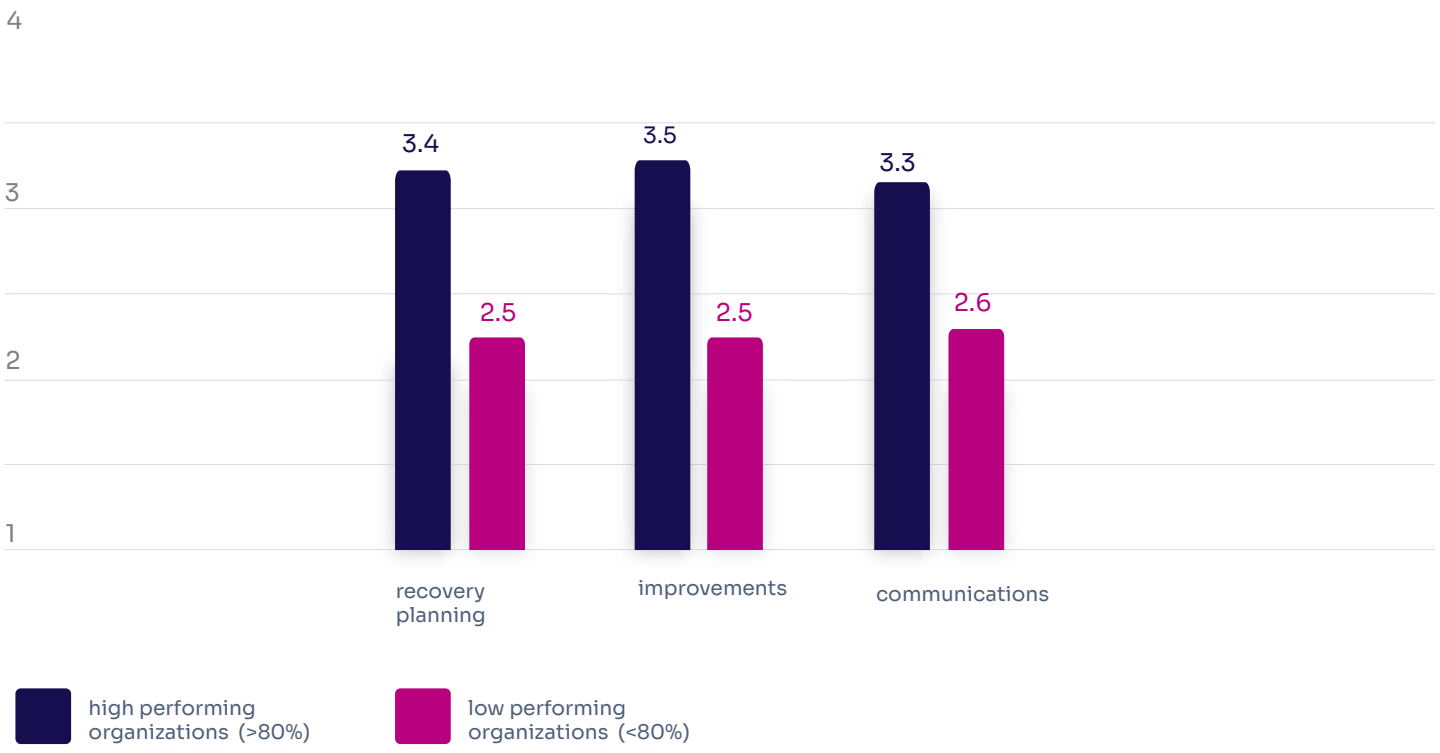
All Low Performers came in at or below

50%

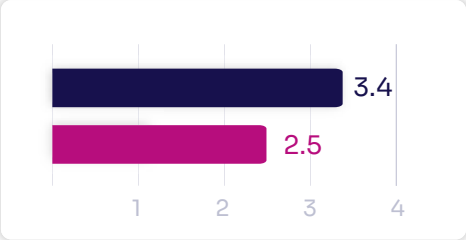
conformance for having an implemented Incident Response Plan.

Recover

Most Boards of Directors and non-IT/Security executives would call Recover the most important NIST CSF function. The Recover Function identifies appropriate activities to maintain resilience plans and rapidly restore any capabilities or services impaired by a cybersecurity incident, returning to a state of normal operations. Despite significant gaps among high performers, we found that they collectively did not disappoint in this category, while low performers are not where they need to be.



Recovery Planning



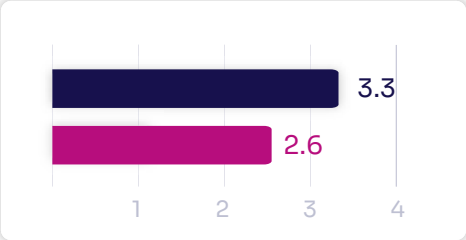
Recovery procedures exist to ensure the timely restoration of systems or assets affected by cybersecurity events. Failure to execute the Recovery plan means nothing will happen; you will not recover. Since 3 represents the minimum level of performance, nearly two-thirds of the organizations in the sector are underperforming in recovery planning.

Nearly

2/3

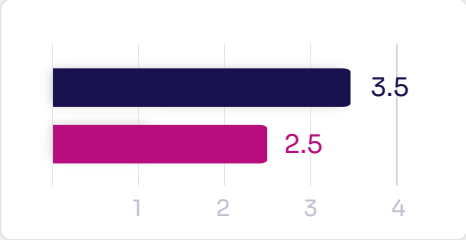
of the organizations are under performing in recovery planning.

Communications



Healthcare is improving across the board in communications. This covers managing public relations, repairing reputation after incidents, and communications with all stakeholders, internal and external, as well as executive and management teams.

Improvement



Improvement is critical in the Recover Function. Externally, threats, and attacks change while internally, your own systems and personnel change. Improvement means incorporating previously learned lessons into the Recovery plan. Most organizations do not start with Respond or Recover, so if you are arriving late to the dance, or if you simply lagging in those two functions, they're good targets for increasing your focus and investment. Faced with the reality that a cyber incident will happen, if you cannot do all the Identify, Protect, and Detect functions, you should at least have Response and Recovery plans, and work to improve them over time.

Update recovery strategies based on your exercises or actual cyber events.

DATA PRIVACY IN 2020

Data Privacy: A Year in Review

Privacy and compliance professionals dealt with a multitude of changes throughout 2020, including:

- New regulatory guidance
- Changes to the data privacy legislation landscape
- The global COVID-19 pandemic

Those responsible for implementing privacy programs and initiatives often faced daunting challenges, including budget cuts, limited resources, staff reductions, and remote working environments, all as potential privacy risks increased due to, newly remote workforces and rapid adoption of telehealth services.

> Organizations with more mature privacy practices are getting higher business benefits than average and are much better equipped to handle new and evolving privacy regulations around the world.
>
> Cisco 2021 Data Privacy Benchmark Study Forged by the Pandemic: the Age of Privacy, January 2021

Regulatory Updates

HIPAA Privacy Updates

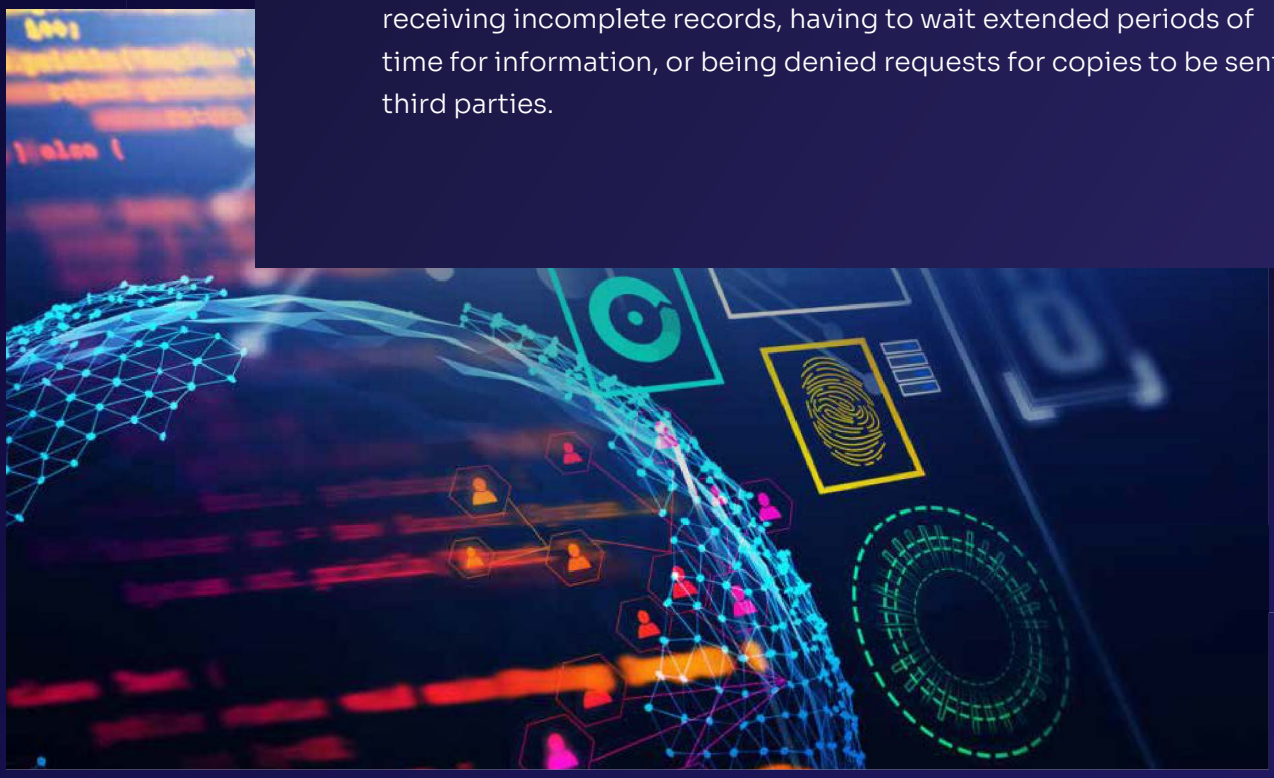
As the federal agency that enforces the HIPAA Privacy Rule, the U.S. Department of Health & Human Services - Office for Civil Rights (OCR), offered some enforcement relief during the pandemic, exercising enforcement discretion and waiving potential penalties for HIPAA violations, including those made in connections with good faith uses of web applications to schedule COVID-19 vaccinations appointments, the use of telehealth remote communications, and operation of community-based COVID testing sites.

Despite the relaxed enforcement, OCR pushed forward with its individual “Right of Access” to health information enforcement initiative by settling 11 related investigations in 2020, and continued enforcement with 18 additional settlement agreements so far in 2021. The HIPAA Privacy Rule requires covered entities to provide individuals with a right to access to inspect and receive a copy of their protected health information (PHI) in a designated record set when requested.

Additional information about OCR’s enforcement discretion and COVID-19 guidance may be found here.

Former OCR Director - Roger Severino - announced this enforcement initiative in early 2019. After announcing the thirteenth related settlement, he said that “OCR created the Right of Access Initiative to address the many instances where patients have not been given timely access to their medical records. Health care providers, large and small, must ensure that individuals get timely access to their health records, and for a reasonable cost-based fee.”

Some of the challenges individuals’ - encountered included - receiving incomplete records, having to wait extended periods of time for information, or being denied requests for copies to be sent to third parties.



OCR's record-breaking 19 total settlements in 2020 extended beyond Right of Access cases to also included covered entities that failed to address OCR compliance assistance and guidance botched implementations of privacy policies, and failures to cooperate with an OCR investigation.

Finally, among other initiatives, OCR issued proposed changes to the HIPAA Privacy Rule in 2020 that would revise the Notice of Privacy Practices acknowledgment requirements and update the response time to access requests. Although covered entities have some time before these changes are finalized, they will add additional demands to already full plates of priorities.

State Attorneys General may bring actions against HIPAA - covered entities and their business associates for HIPPA Rule violations with damages ranging from $100 per HIPAA violation up to a maximum of $25,000 per violation category, per year. There were no reported fines or actions in 2020, but organizations should be prepared for increased enforcement activity as states begin to effectively control the spread of COVID-19.

Ninety-three percent of organizations are reporting privacy metrics (e.g., privacy program audit findings, privacy impact assessments, and data breaches) to their Boards.

Cisco 2021 Data Privacy Benchmark Study Forged by the Pandemic: the Age of Privacy, January 2021

Enforcement details and agreements may be found here.
More information about the proposed modifications may be found here.

State and Federal Data Privacy Law Update

State Data Privacy Laws

California's Consumer Privacy Act (CCPA) is probably the most widely known state privacy law, becoming effective in January 2020 - around the same time the first COVID-19 cases were reported in the United States. Initial CCPA regulations were approved in August 2020 - and nearly one year later, compliance remains challenging for covered businesses. California residents now have certain CCPA rights in their personal information, and certain businesses must meet obligations regarding collection of California residents' personal information. Additionally, the California Consumer Privacy Rights Act (CPRA) was approved in November 2020, further expanding consumer privacy protections for California residents. Many of the CPRA's provisions become effective on January 2, 2023.

Privacy professionals also watched closely as several new consumer data privacy state laws were introduced in 2020. New Hampshire, New York, and Oregon introduced and referred data privacy legislation to committees. Thirty states, (including Florida, Illinois, and Washington), tried and failed to pass data privacy legislation. Texas and Connecticut established task forces to examine data privacy practices in businesses and make legislative recommendations. Although these states failed in passing data privacy laws, it is only a matter of time before other states follow California's lead. Eleven states have introduced data privacy laws in the first few months of 2021.

Despite other states' struggles to pass data privacy laws, Virginia enacted the Virginia Consumer Data Protection Act (VCPDA) in March 2021. VCPDA goes into effect on January 1, 2023, applying to certain businesses collecting personal information from Virginia residents, and grants Virginians certain rights similar to the CCPA and CPRA.

Additional information about the CCPA requirements may be found here.
Read more about the VCPDA's requirements here.

Federal Data Privacy Laws

As in prior years, Congress has struggled to implement a federal privacy law that would go beyond the HIPAA's requirements to include personally identifiable information. Congress introduced The Consumer Data Privacy and Security Act (CDPSA) in March 2020, then the Setting and American Framework to Ensure Data Access, Transparency, and Accountability Act (Safe Data Act) in September 2020. Similar to other data protection laws, CDPSA and the Safe Data Act proposed guarantees of certain individual rights, while requiring the appointment of privacy officers and assessments of annual privacy impact.

Although passing federal privacy legislation remains challenging largely due to disagreements over whether the legislation should include a private right of action, a federal data privacy law looms in our future. Since information about consumers has quickly become the lifeblood of the digital economy, consumers have demanded rights and protections. As a result, if Congress and state legislatures believe companies are not sufficiently protecting the privacy of personal data or providing certain rights related to that data, increased regulation will likely follow.

In addition, privacy, compliance, and information security professionals raced to implement the 21 st Century Cures Act Final Rule before it's April 5, 2021 compliance date. Issued by the federal Office of the National Coordinator for Health Information Technology, the Rule prohibits information blocking about patients and others unless an exception applies. Any person or entity subject to the Rule needs to determine where electronic health data is located, update access policies and procedures, determine whether sharing exceptions apply, assess related vendor contracts, and provide staff training.

More information about the Information Blocking Rule, including factsheets, FAQs, and webinar recordings, may be found here and on CynergisTek's website.

2020 HIPAA Privacy Program Results

Even though many of our healthcare organizations implemented HIPAA privacy programs a decade or more ago, our analysis underscores further opportunities for organizations to improve, as well as where many have made tremendous progress.

Focus for 2021

Challenge Area	How to Address
No or limited user access monitoring and auditing	Utilize a tool, and risk-based methodology to assist in performing proactive versus reactive monitoring
Defective HIPAA authorizations	Ensure both the authorization template and authorization policy describe the core elements and required statements
Violations of the Minimum Necessary Rule	Define criteria to limit the PHI disclosed and request the amount necessary to achieve the purpose of the disclosure
Insufficient policies and procedures	Implement policies that are updated and appropriate versus keeping them in draft form
No or inappropriate Hybrid Entity designation	Perform covered and non-covered functions and accurately designate health care component(s).

Positive Results in 2021

Organizations are improving or creating new privacy policies and procedures that more accurately comply with rules, laws, and best practices.

Organizations saw significant improvements to CynergisTek's privacy compliance score (in some cases resulting in an improvement from 45% to 85% compliant). by remediating defects to Notices of Privacy Practices, as well as updating policies and practices. addressing the Breach Notification Rule (among others)

Organizations are requesting assessments and services to address data privacy beyond HIPAA and PHI, including data that is subject to other rules, laws, controls, and frameworks.

Organizations are addressing gaps in their user access monitoring and auditing program by implementing new tools, practices, and revision policies.

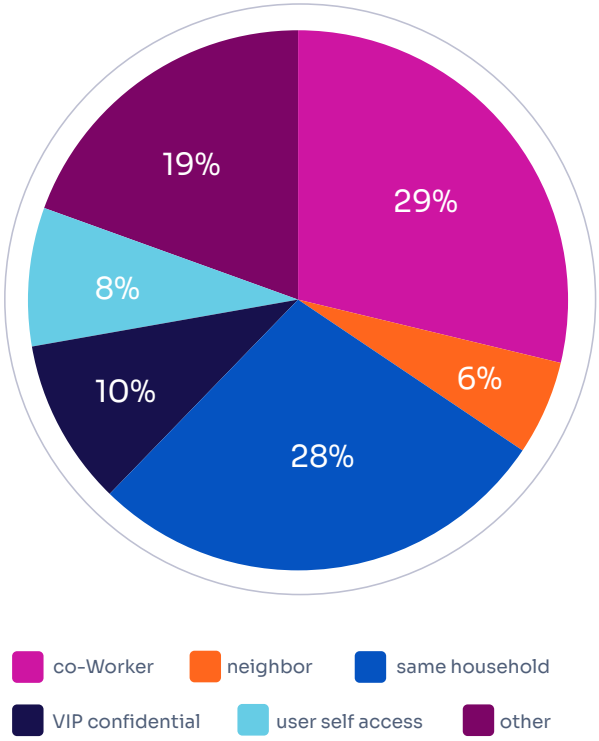
2020 User Access Monitoring Results

CynergisTek's Patient Privacy Monitoring Service (PPMS) analysts analyzed approximately **two million lines of data and hundreds of thousands of user/patient accesses** within a variety of user access monitoring tools. Using CynergisTek's PPMS, organizations connected with a team of expert privacy analysts, who reviewed all escalations and violations via tools, as well as upon request.

Escalations and Violations

- Escalated less than 5% of accesses reviewed, which allowed privacy and compliance offices to focus on other vital privacy initiatives.
- Routinely reviewed co-worker, same address, same street, same unit, self-access, VIP, and other reports/violations
- The highest rates of applied sanctions in 2020 involved same household, user self-access, and same last name case types.

Report Types



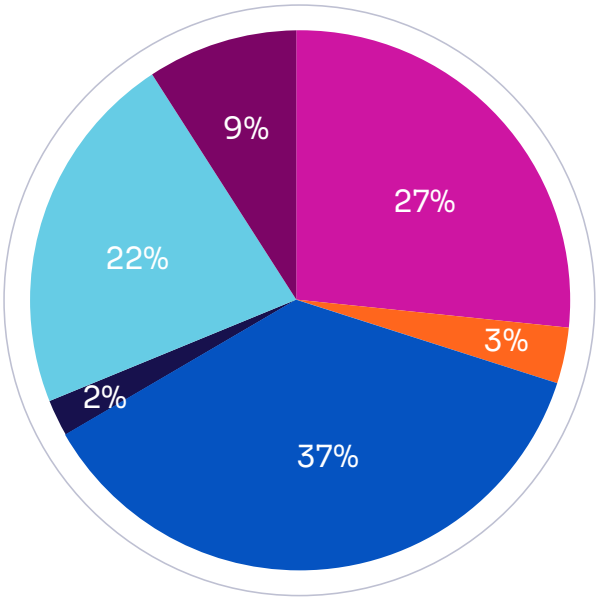
User Self-access Data

PPMS analyzed approximately 122,100 audit rows and identified approximately 2,865 users who accessed their own records. If a policy was present to restrict self-access, **there would have been 2,865 incidents to investigate and may have resulted in sanctions.**

Types of Unauthorized Access

Types of events monitored to detect and identify suspicious activity:

Types of Unauthorized Access Events



PRIVACY
EXECUTIVE TAKEAWAYS

The four key data privacy and OCR enforcement industry trends:

1 State-by-State Privacy Legislation.

While breach notification laws can be found in every state, privacy legislation continues to move – albeit slowly – forward. California, Colorado, and Virginia now have data privacy and related consumer protection to safeguard the privacy of their residents. As of the summer of 2021, a majority of states have introduced data privacy legislation. In addition, the United States, as well as a variety of other countries continue to work towards a consensus regarding standardizing of data privacy practices. Organizations should continue to closely monitor the effect of state and international privacy and consumer protection laws as we anticipate other states will follow California, Colorado, and Virginia in finalizing privacy legislation.

2 Right of Access.

In 2020, OCR settled 11 cases to resolve violations of OCR's HIPAA Individual Right of Access initiative. This initiative is focused on compliance with the HIPAA Individual Right of Access, which requires covered entities to respond in a timely manner to requests from individuals to their protected health information (PHI) for only a reasonable, cost-based fee. As there is no indication that OCR intends to discontinue this initiative, covered entities should verify policies and processes are in place to appropriately respond to requests for access to PHI.

3 Patient Treatment and Safeguards Post-COVID-19.

According to the Centers for Disease Control (CDC), during the first quarter of 2020, the number of telehealth visits – most patients seeking care for conditions other than COVID-19 - increased by 50%, (compared with the same period in 2019), with a 154% increase in visits noted in week 13 in 2020, compared with the same period in 2019. As this not-so-new technology became more ubiquitous in 2020, it is very likely some of the trend towards telehealth over in-person visits will become more prevalent. As providers shift to telehealth visits, the workforce must be trained on policies and procedures for safeguarding the privacy of individuals who chose to use telehealth services.

4 Continued Focus on Business Associates.

In September 2020, OCR announced a $2.3 million settlement with CHSPSC LLC (CHSPSC), a business associate providing services including IT and health information management, to certain hospitals and physician clinics. Since 2013, OCR has not been shy about investigating both business associates and relationships between covered entities and their business associates. In addition, as HIPAA is not very prescriptive regarding responsibilities of a covered entity to monitor, audit, or otherwise examine compliance activities of its business associates, organizations continue to be challenged to implement policies and practices regarding oversight of vendors and business associates.

ACTION
DRIVES CHANGE

As our report shifted from scores to data-based guidance, our top organizational recommendation this year is to continuously reduce cyber risks while adapting to business, technology, and regulatory changes. Security remains a journey, rather than a destination, and there is no stopping until threat actors decide to leave healthcare alone. If that didn't happen during the COVID-19 pandemic, it's not going to happen.

Given current trends, healthcare organizations need to focus on the following areas:

1

Automate security functions.

Security automation can detect, investigate, and even remediate cyber events and threats in near-real-time, with or without human intervention. While you will need tools with artificial intelligence and machine learning, you can have too many tools, including ones that overlap, and others that claim to integrate with one another, but actually don't. So tread carefully: Anything that says it will solve everything will not, and acquiring enough individual tools to actually solve everything may well destroy your budget and leave you understaffed. The wise move is to prioritize, focusing on automations that can be manually diagrammed, then adopt automation gradually, and invest in training to be sure your chosen tools and automation is being used properly.

2

Validate technical controls for people and processes.

Several years ago, testing for organizational system and network weaknesses was a new concept; now there are multiple tools to validate a layered security infrastructure's overall effectiveness, finding gaps and flaws that people or automated processes missed. Unfortunately, technology validation usually begins with technologies rather than threats, so as time passes and threats change, both technologies and the people who use them may not be as effective as when they were originally deployed. Validating technical controls for people and processes means that when an alert fires, it goes to the right people, and they follow current procedures on what to do when they get that alert. This technical control validation process ensures that everything works as you want it to, now.

As Aristotle said, "we are what we repeatedly do. Excellence, then, is not an act but a habit." American golfer Sam Snead put it another way: "Practice puts brains in your muscles." The same lessons apply to security, especially cybersecurity.

3 Perform exercises and drills at the enterprise level, testing all components of the business.

If you want to have an effective response when the "boom" happens, do what the military and hospitals do: Practice, on a large scale, before you're faced with an actual crisis. After you have practiced, build all the lessons you learned into the next rehearsal. Sometimes it really is that simple – do it, do it again, then repeat.

4 Secure the supply chain.

As the Cybersecurity Infrastructure & Security Agency puts it, the "supply chain is only as strong as its weakest link... Constant, targeted, and well-funded attacks by malicious actors threaten government and industry alike by way of their contractors, subcontractors, and suppliers at all tiers of the supply chain." As you dive into this report, you will find that the supply chain was the weakest category across the board; whether suppliers became targets themselves, or served as tools for bad guys to exploit enterprise organizations, supply chain issues exploded during COVID-19. This area must be addressed quickly and effectively: The healthcare sector is already lagging in overall security investment, and lagging even further in the most rapidly growing threat category is profoundly dangerous.

5 Privacy must look to and beyond regulatory requirements.

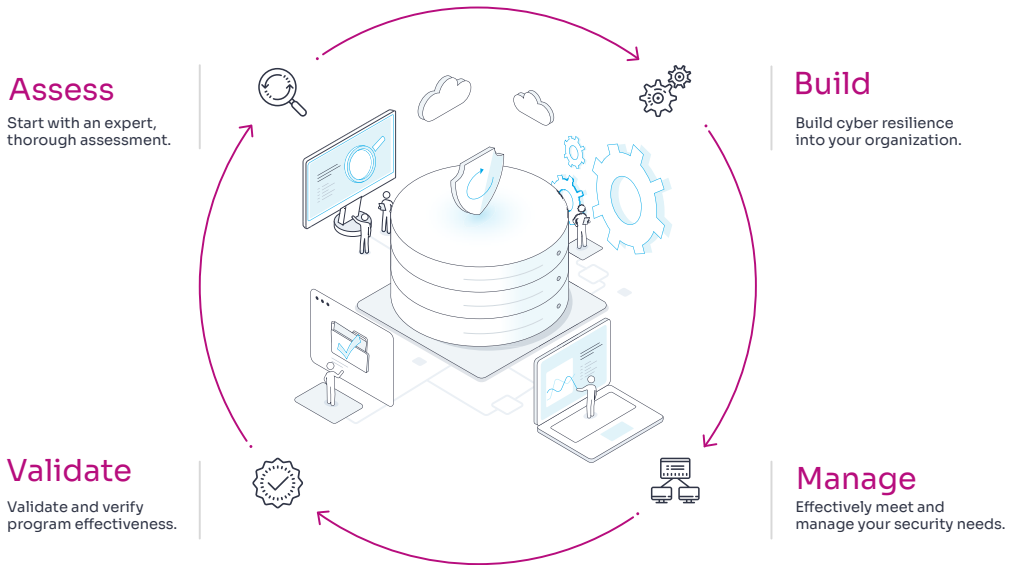
As privacy, security, and compliance professionals continue to further enhance their organizations' risk and compliance posture in 2021 and beyond, it will be imperative to look beyond regulatory requirements as they seek to evaluate potential consequences for consumer privacy. Failure to properly identify data received, maintained, or transmitted, (and to also consider whether all data collected is necessary) can have adverse consequences for both an individual's privacy and the organization's ability to maintain trust and growth. Organizations should consider implementing structures, such as individuals and groups responsible for data governance, as well as mechanisms to appropriately respond to requests from consumers, patients, and others seeking to exercise certain rights related to data about them.

Conclusion

The advice we issued in our 2020 annual report was sound at that time and held through the year, though there's one phrase we would have changed in retrospect: "economic downturn following COVID-19" would more accurately have read "economic impacts." While the pandemic impacted every organization's cybersecurity budget and spending, those numbers varied based on multiple reasons, including (and in some cases despite) the organization's own overall financial standing.

Going forward, it's clear that this isn't the right time to cut back on cybersecurity, and that smart spending will be necessary to secure organizations against a rising tide of ransomware threats against critical infrastructure generally, and healthcare specifically. As we ride out the remainder of 2021, it's within your power to ensure that the economic impacts of the digital transformation on your organization are net positive – assuming you make the right, proactive decisions to protect your assets and environment now.

CynergisTek's Resilience Validation™ methodology helps organizations prepare, rehearse and validate their security, privacy, and compliance programs are working and responding effectively to risk every day. At CynergisTek, we understand strong, mature programs aren't developed overnight. We provide customized service offerings categorized under the four pillars of Asses, Build, Manage, and Validate that align with your organization's immediate, and long-term goals. Our experts evaluate your unique needs and provide your team and organization guidance on your journey to ensuring your programs have a security, privacy, and compliance approach that is resilient against threats.



Contact us Today →

BE READY. BE RESILIENT. VALIDATE.