AON'S 2021 CYBER SECURITY RISK REPORT

Balancing risk and opportunity through better decisions

Cyber risk runs deep.
Is your organization making informed decisions around its cyber budget?

Aon's 2021 Cyber Security Risk Report helps answer this question.

AON

Table of Contents

Foreword

Now more than ever, global leaders are finding themselves under increasing pressure. Revenues are down, budgets are constrained, and the continuous rush to transform has organizations playing catch-up in the cyber security game. All of which means that tougher decisions need to be made in increasingly complex environments.

Across industries, the velocity of digital change outpaced that of security in 2020; with organizations giving up ground to keep the lights on and maintain momentum. The majority of the cyber threats organizations face today are not new – connected devices, ransomware, and insider risk will be ever-present. But what is new is that COVID-19 ushered in a 360-degree shift in the nature of business and exponentially intensified cyber risk. This was seen by a sharp uptick in the number and severity of ransomware cases, coupled with supply chain and support vendor vulnerabilities.

Successful cyber attacks that came to light at the end of 2020 and start of 2021 — including Mimecast, SolarWinds, Accellion, and Microsoft Exchange —highlighted vulnerabilities associated with working with third-parties. Ransomware became a headline risk for insurers and insureds alike, as activity grew dramatically — up 400% from the first quarter of 2018 to the fourth quarter of 2020.[1] Underwriters, who saw their cyber insurance portfolios running at a loss predominantly due to ransomware, recognized the critical need to better evaluate and put a higher price on cyber insurance.

The challenges are profound and run deep. Global organizations are not in a state of digital transformation — this term implies a beginning, middle and an end. What organizations are experiencing is digital evolution, and new risks are emerging daily.

It is a balancing act between risk and opportunity, and organizations are constantly asking themselves: **How can we make informed decisions around our cyber budget to support changing business models – while protecting our people, clients, partners, and our balance sheet?**

Against this backdrop we deliver **Aon's 2021 Cyber Security Risk Report: Balancing risk and opportunity through better decisions**, our annual analysis of the state of cyber risk. This report concentrates on four key risks that are critical today, entitled: *Navigate new exposures*, *Know your partners*, *Concentrate on controls* and *Perfect the basics*, and closes with a discussion on emerging risks. Using our leading-edge data, analytics, and expert insights, the report aims to help organizations evaluate their cyber risk maturity and make better enterprise risk decisions.

New this year is insight derived from Aon's Cyber Quotient Evaluation (CyQu), a cyber risk assessment that evaluates cyber risk maturity across nine security domains. CyQu helps organizations understand cyber threats through both a commercial and information security lens. The 2020 data tells us that organizations, across various regions, industries, and revenue bands are on average performing under baseline – and only maintaining a basic level of cyber maturity and readiness.

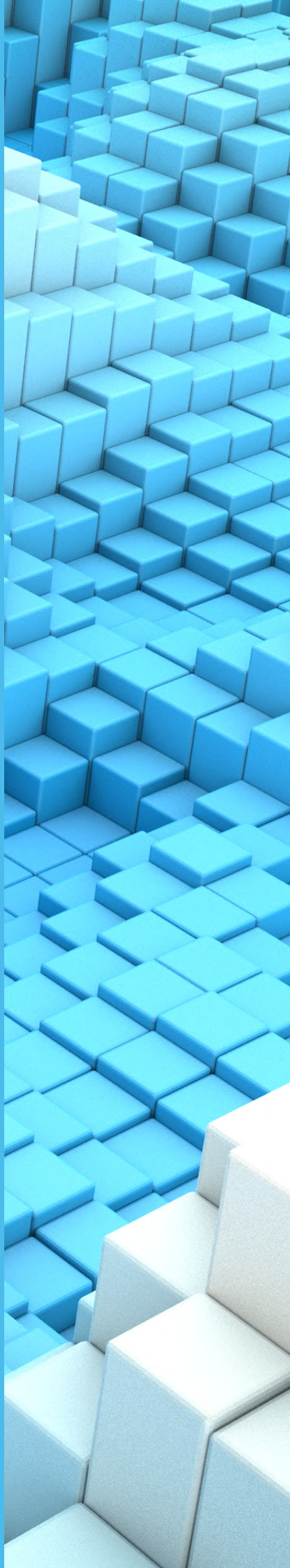
A case in point, only two in five organizations report that they are prepared to navigate new exposures arising from rapid digital evolution. More alarmingly, a mere 17% of organizations report having adequate application security measures in place. Moving to third-party risk, only 21% of organizations report having baseline measures in place to oversee critical suppliers and vendors. Overall, the CyQu data tells us that cyber security risk management practices and technologies are not formalized, and that risk is being managed in an ad hoc and reactive manner.

Throughout 2021 and beyond, organizations have much work ahead to pass the scrutiny of regulatory bodies, insurers, partners, and customers. This report will help empower results, and guide organizations as they evolve towards managing cyber risk as an enterprise risk.

Methodology

Data on security performance trends were drawn from Aon's Cyber Quotient Evaluation (CyQu), an online cyber risk assessment. 996 organizations representing 20 industry groups and spanning North America, Europe, Middle East and Africa, and Asia-Pacific, provided data. More than 111,552 data points were recorded, and security performance trends were structured using the nine security domains and 35 critical control areas that comprise the CyQu methodology.

Cyber risk themes



Navigate new exposures: **Rapid digital evolution**

Step aside CTO, CIO, and CFO. COVID-19 joined the C-suite in 2020, leading change as companies were forced to rapidly set up remote work environments and enable digital customer experiences.

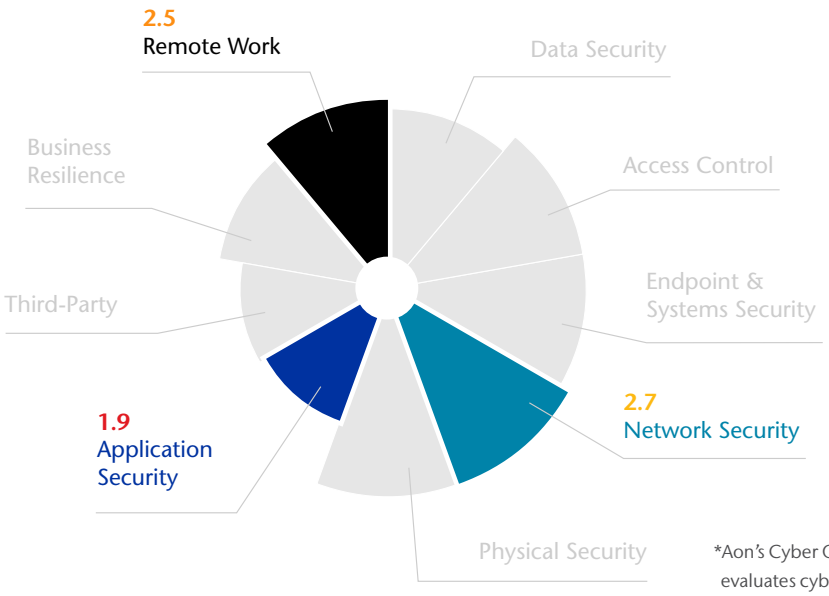
Any thought of a paced and strategic digital agenda was tossed aside in favor of survival. Perhaps your company rapidly transitioned to the cloud. Under time and cost pressures you execute a 'lift and shift' approach, quickly moving existing architecture to a new cloud environment. You may now believe that this strategy, necessary as it was, brought considerable security disadvantages and perhaps offset the many benefits of the cloud. Or, your organization weathered the pandemic, but the board is now calling for more innovation; maybe urging deployment of Artificial Intelligence (AI) to inform smarter decisions.

Change seems constant, and it is. Organizations are in a process of digital evolution. The continued drive towards innovation, for example the Internet of Things (IoT), Internet of Bodies (IoB), and Smart City initiatives, will continue to pose yet more cyber risk in 2021. Operating in this environment, organizations are called on to weigh the projected benefits of a digital agenda against the cyber risk introduced by adopting new technologies or business models.

As part of an enterprise-wide approach, it is essential to identify the cyber risks and threats; mitigate risks as appropriate through best cyber security practices; prepare and be ready for incidents; and consider which part of the risk to transfer off the balance sheet through insurance, and then scrutinize current and available policies to ensure new risks are covered.

Organizations are challenged to navigate the new exposures arising from rapid digital evolution.

Key risks arising from **rapid digital evolution**



CyQu Scoring

Initial
1 - 1.9

Basic
2 - 2.5

Managed
2.6 - 3.4

Advanced
3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu) is a cyber risk assessment that evaluates cyber risk across 9 security domains and 35 critical control areas.

Remote Work

CyQu global average | **2.5 (Basic)**

Enables users to remotely access corporate systems and data securely to deliver on their roles and responsibilities when outside of corporate working environments.

See page 34 for score description.

Remote working is here to stay, yet only **40%** of organizations report having adequate remote work strategies to manage this risk.

These measures include:

- Remote Connectivity
- Authentication and Identity
- Device Vulnerability and Monitoring
- Remote Business Continuity
- Remote Security Awareness

Application Security

CyQu global average | **1.9 (Initial)**

Protects applications from threats by requiring measures or checks during each stage of the application development life cycle.

See page 34 for score description.

Only **17%** of organizations report having adequate application security measures in place for the rapid pace of digital evolution.

These measures include:

- Training
- Secure Development
- Software Management

Close the gaps

Organizations that are not adequately managing application security risks should consider secure development security training for all developers, and perform application penetration testing on critical digital service.

Network Security

CyQu global average | **2.7 (Managed)**

Delivers infrastructure services including enterprise defence for network, compute, physical presence, cloud, storage management and operations.

See page 34 for score description.

Positively **60%** of organizations report having sufficient network security measures in place to manage new digital connectivity.

These measures include:

- Network Environment
- Wireless Security
- Network Penetration Testing
- Network Capacity

Know your partners: **Third–party risk**

The time is now to double down on your security. This year, expect dark lines to be drawn. Organizations will evaluate the cyber risks arising from their supply chains in new ways and with heightened concern.

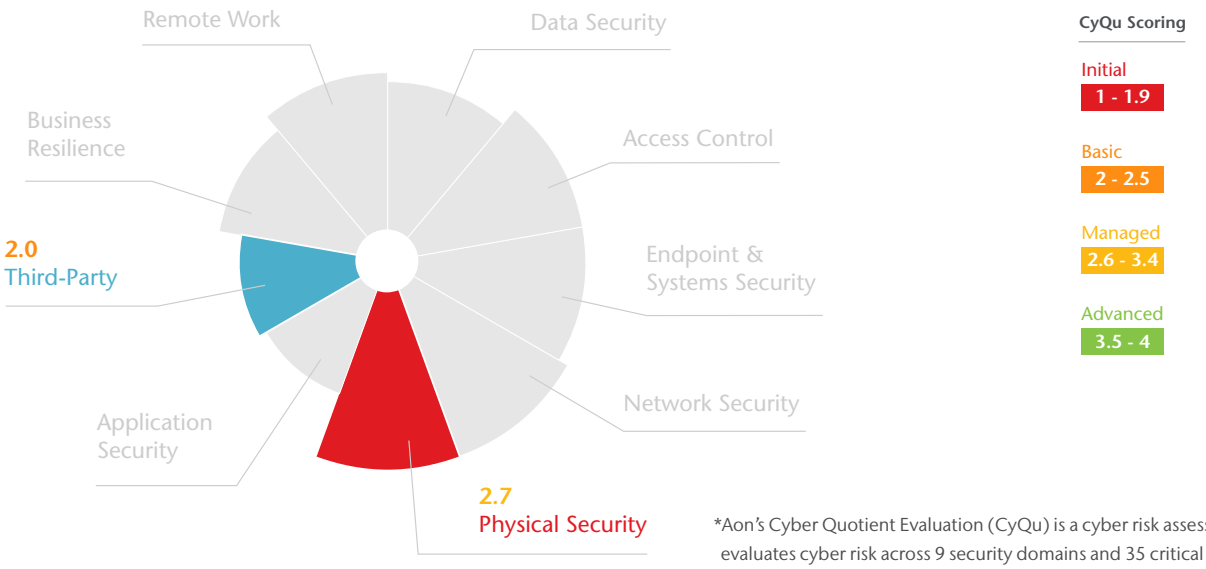
If certain standards cannot be met, contracts will not be signed. The reasoning is simple. It takes just one undefended back door to compromise business viability – most recently illustrated by the supply chain compromising Accellion's legacy file-sharing program, and SolarWinds' Orion network management software.

For-profit, non-profit, academia, government – all organizations are interconnected, and COVID-19 forced more dependency on third-parties as organizations scrambled to meet digital demands. The march towards Central Processing Units (CPUs) and hybrid computer chips with software components is also ushering in new risk. Compromise one version of a chip, and a hacker now has potential access to thousands of organizations. Even knowing all of this, organizations may be hard-pressed to actually assess the vulnerability and security of their supply chains. The static approach of relying on the unverified and untested responses supplied to a 500-question risk assessment may no longer be enough.

So, what can your organization do? Third-party source code review may be an option but will likely be resisted and beyond the abilities of many. Assessments and certifications by trusted neutral third-parties may become best practice. A comprehensive controls assessment, combined with risk quantification and insurance planning, is a start. But managing third-party risk truly demands a continuous assurance model, with ongoing cyber scanning and threat hunting, for example via red teaming. Organizations must also become prepared to respond, and are tasked with choosing the right incident response vendor. Quality varies, and insurers are demonstrating less flexibility in the use of non-panel or pre-agreed vendors.

Organizations are not ready to assess and manage third–party risks.

Key risks arising from **supply chains**



*Aon's Cyber Quotient Evaluation (CyQu) is a cyber risk assessment that evaluates cyber risk across 9 security domains and 35 critical control areas.

Third-party

CyQu global average | **2.0 (Basic)**

Monitors relationships with third-parties to ensure provided services adhere to defined security policies.

See page 34 for score description.

An alarmingly low **21%**, or **one in five** organizations, report having adequate third-party management measures to oversee critical suppliers and vendors.

These measures include:

- Third-Party Contracts
- Due Diligence
- Third-Party Inventory

Close the gaps

Organizations that are not adequately managing third-party risks should consider a range of due diligence, onboarding, and contract risk management measures. Perform cyber security assessments on third-parties during the vetting stage, and onboarding processes. Require third-parties to agree to Service Level Agreements (SLAs) to periodically perform cyber security assessments, penetration testing, and business continuity management and response exercises.

Physical security

CyQu global average | **2.7 (Managed)**

Protects facilities, equipment, resources, and personnel from unauthorized access, damage or harm.

See page 34 for score description.

Positively **60%** of organizations report having adequate physical security strategies.

These measures include:

- Physical Access
- Physical Penetration Testing
- Tampering and Alteration Controls
- Environmental Controls

Concentrate on controls: **Ransomware**

COVID-19 added fuel to an already burning fire, as the number and variety of ransomware attacks exploded in 2020. Cyber insurers reported a 336% jump in claims from the start of 2019 through to 2020.[3]

Business costs associated with ransomware are expected to reach USD 20 billion in 2021.[4] Ransomware is no longer confined to the simple model of 'pay to decrypt', and data may be extorted, breached, or even erased. Business interruption is highly likely.

At the close of 2020, seven in ten ransomware attacks involved the threat to leak exfiltrated data,[5] and some variants threatened to auction stolen data. There was also an emergence of data destruction, in which servers or clusters of data are permanently wiped.[6] On top of ransomware, 2021 will present ongoing risk from criminals funded by foreign nation states in their private enterprise hacking that aligns with state-sponsored activities and interests.

The most severe threat will continue to be Advanced Persistent Threats (APTs), which introduces yet another challenge and a substantial compliance burden: knowing the risks of payment when the attacker could be a potential 'bad actor' under government sanction. All of this complexity is not lost on insurers. Many cite ransomware as a major factor impacting their cyber insurance loss ratios,[7] and 62% of underwriters cite access control as a critical topic.[8]

So what should your organization do? It is critical to demonstrate concrete risk mitigation actions, or organizations might be subject to sky-high cyber premiums. Take steps to reduce your organization's exposure footprint, and minimize the impact of data exfiltration. Retain only qualified cyber security professionals to identify vulnerabilities, establish business continuity plans, and assist with breach response.

Most organizations fail to concentrate on the right controls to prevent and respond to ransomware attacks.

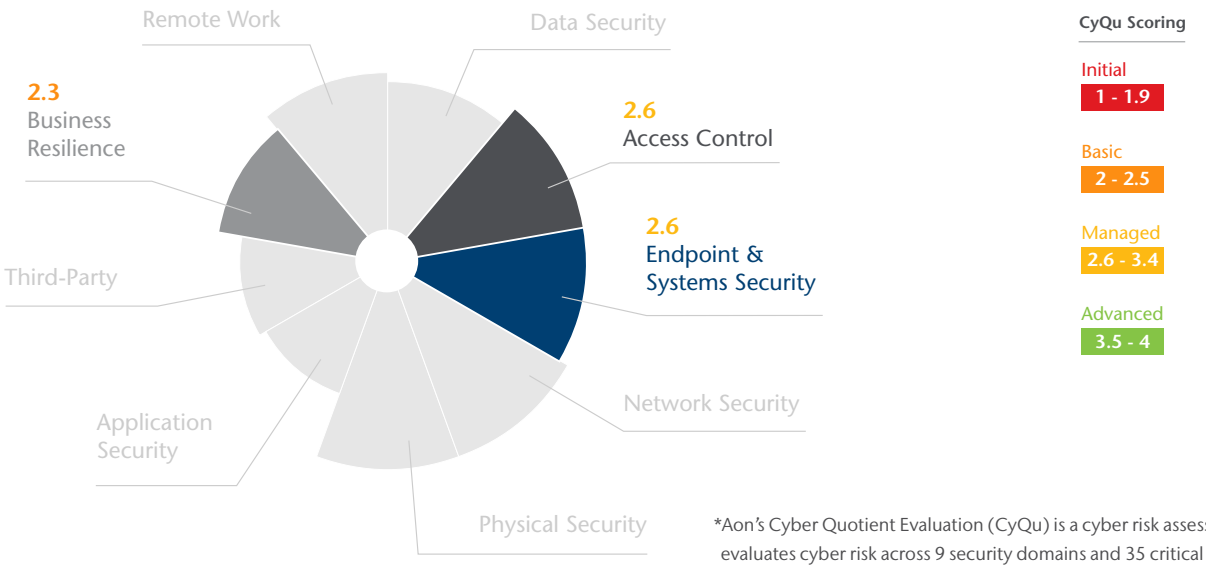
Many hover dangerously close to being at an initial – or nascent – stage of risk maturity.

July 23, 2020[2]
Multinational Technology Company, worldwide outage.
Ransom paid: USD 10M.

July 27, 2020
Business Travel Management Company, 30,000 computers taken down and confidential business files stolen.
Ransom paid: USD 4.5M.

December 31, 2020
Worldwide Money Management Company, accessed, copied and encrypted 5GB of data.
Ransom paid: USD 2.3M.

Key risks arising from **ransomware**



*Aon's Cyber Quotient Evaluation (CyQu) is a cyber risk assessment that evaluates cyber risk across 9 security domains and 35 critical control areas.

Access control

CyQu global average | **2.6 (Managed)**

Grants authorized users the right to use a service while preventing access to non-authorized users.

See page 34 for score description.

44% of organizations report having adequate access management measures in place, yet insurers see this control as critical.

These measures include:

- Two-Factor Authentication
- Password Configuration
- Access Management

Endpoint & systems security

CyQu global average | **2.6 (Managed)**

Delivery and administration of infrastructure services, systems monitoring, endpoint protection, configuration management, storage management and infrastructure operations.

See page 34 for score description.

Positively **49%** of organizations report having sufficient endpoint & systems security.

These measures include:

- Endpoint Protection
- Vulnerability Management
- Asset Inventory
- Secure Configuration
- Logging and Monitoring

Business resilience

CyQu global average | **2.3 (Basic)**

Plans for prompt and effective continuation of business critical services in the event of a disruption.

See page 34 for score description.

Ransomware poses a business interruption and balance sheet risk, but only **31%** of organizations report having adequate business resilience measures in place.

These measures include:

- Business Continuity and Disaster Recovery
- Incident Response
- Backup

Close the gaps

Organizations that are not adequately managing disruptive cyber risks should consider a business continuity strategy that encompasses analysis, planning, testing, and governance. It is critical to build a Business Continuity Plan (BCP) that explicitly addresses disruptive cyber risk scenarios that consider both internal technology, and third-party services.

Perfect the basics: **Regulation**

Businesses in 2020 wrestled with understanding if, when, and how they should invest in achieving compliance. Actions varied wildly across industries and revenue segments.

The rapid changes forced by COVID-19 only served to broaden pre-existing compliance gaps, and potentially generate new ones. A fictional, but entirely realistic example could be a healthcare organization that may have swiftly launched telemedicine to save lives, and in doing so may have brushed off some elements of HIPAA compliance. Or a retailer that might have signed a dozen third-party contracts to rapidly scale a digital storefront, forgoing cyber security due diligence. Now is the time to fix past missteps and perfect the basics to ensure future success.

Entering 2021, change is underway. Impelled by the SolarWinds breach, United States President Joe Biden proposed USD 9 billion in funding to bolster the work of the country's Cyber Security and Information Security Agency (CISA). Section 230 of the US Communications Decency Act is likely to be revisited, as individuals across both sides of the political divide want to know that technology companies are accountable.

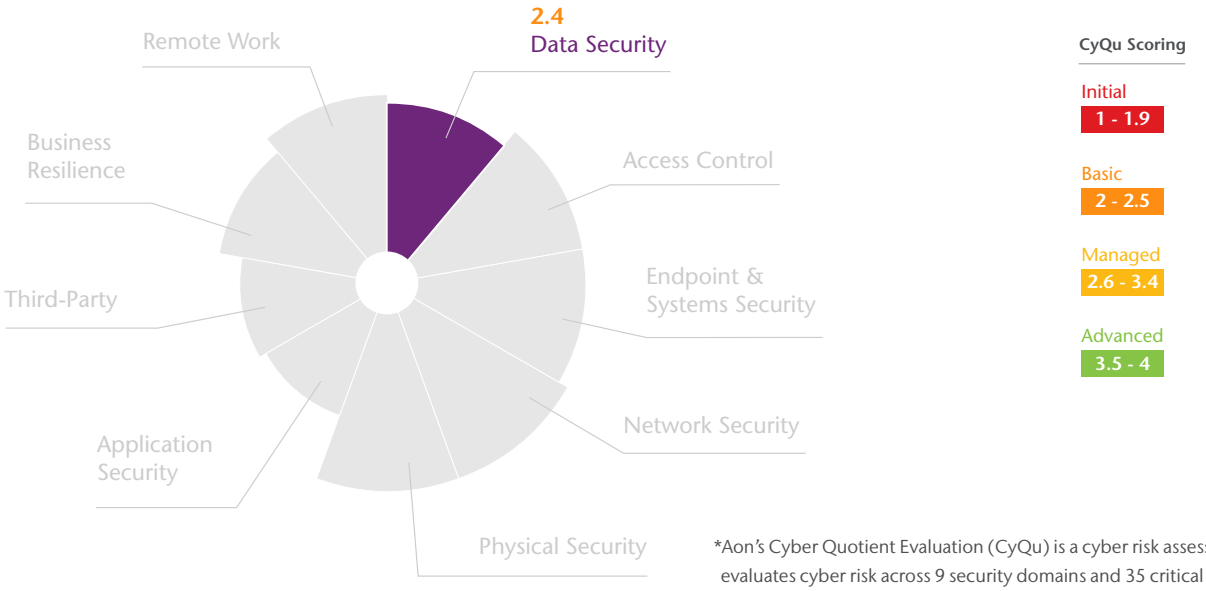
Additionally, falling into line with the European Union's General Data Protection Regulation (GDPR) needs to be a centerpiece of any cyber security plan. Data privacy regulation mirroring GDPR will continue to emerge, and in May 2020 we saw Thailand's Personal Data Protection Act (PDPA) take effect. Similarly, the US California Privacy Rights Act (CPRA) became law at the end of 2020, expanding and amending the original California Consumer Privacy Act (CCPA), to become the most restrictive data protection law in the US.

As the digital evolution intersects with medicine, the healthcare industry will see more regulatory demands. The new EU Medical Device Regulation (MDR) is mandatory, and requires manufacturers to take into account principles of risk management, including information security, as well as protection against unauthorized access.

It is complicated at best, and organizations navigating regulatory risk must be mindful. Compliance does not equate to security; the standards just set the baseline. Best security practices will require bespoke solutions based on specific business needs and activity, and may extend past governing standards.

Organizations have yet to perfect the basics when it comes to managing current and pending regulatory challenges.

Key risks arising from **compliance gaps**



*Aon's Cyber Quotient Evaluation (CyQu) is a cyber risk assessment that evaluates cyber risk across 9 security domains and 35 critical control areas.

Data security

CyQu global average | **2.4 (Basic)**

Manages safeguards to protect the confidentiality, integrity, and availability of information.

See page 34 for score description.

Less than **two in five** organizations (**36%**) report they have adequate levels of data security preparedness.

These measures include:

- Data Classification
- User Awareness and Training
- Data Protection
- Governance
- Risk Management

Close the gaps

Organizations that do not have adequate risk management approaches for data privacy and regulations should consider integrating data privacy and cyber security regulatory risk into the enterprise risk management framework. Appoint an executive-level champion, e.g. CIO, CISO, or GC, to sponsor and promote cyber security matters to the board.

How does your **industry** stack-up?

Industry insights
Construction

Heavily reliant on delivering projects on a timeline, construction organizations are prime targets for ransomware attacks that have the potential to disrupt business. There is also the risk of Intellectual Property (IP) theft of sensitive blueprints, as well as a potential breach of AI-powered autonomous vehicles. While the construction industry has historically avoided the cyber risk spotlight, vulnerabilities are increasing.

How does the **construction** industry stack up?

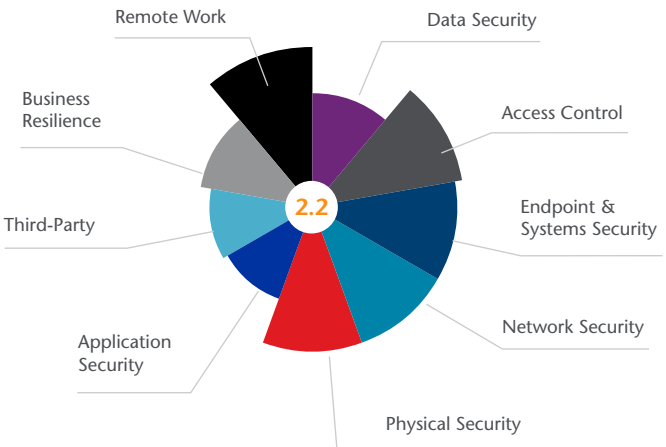
2.2 (basic)

The average CyQu rating for construction organizations globally is 2.2/4 (basic).

What this means

This rating indicates that cyber security maturity is at a basic level. Organizational cyber security risk management practices and technologies are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. Risk management practices and technologies are not established organization-wide.

Explore the most pertinent cyber risks to construction organizations, map them to key cyber security controls, and determine actions your organization can take to close cyber security gaps.



Security Domain	Industry Average	Global Average	
Rapid Digital Evolution			
Network Security	2.4	2.7	↓
Application Security	1.6	1.9	↓
Remote Work	2.6	2.5	↑
Third Party			
Physical Security	2.4	2.7	↓
Third-Party	1.7	2.0	↓
Ransomware			
Access Control	2.5	2.6	↓
Endpoint & Systems Security	2.4	2.6	↓
Business Resilience	1.9	2.3	↓
Regulations			
Data Security	1.9	2.4	↓

CyQu Scoring

Initial 1 - 1.9

Basic 2 - 2.5

Managed 2.6 - 3.4

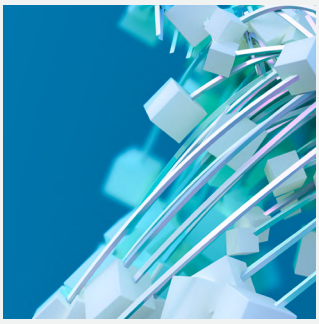
Advanced 3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu) is a cyber risk assessment that evaluates cyber risk across 9 security domains and 35 critical control areas.

Underpinned by proprietary data and expert insights, explore four key risk themes that are prominent to **construction** organizations today.

Navigate new exposures: **Rapid digital evolution**

More than half (**57%**) of organizations do not undertake any form of penetration testing. This is not surprising, given the perception within construction that cyber risk is less critical for them. As this industry digitally matures, cyber risk will be more visible, and controls will need to be maintained.



Know your partners: **Third-party risk**

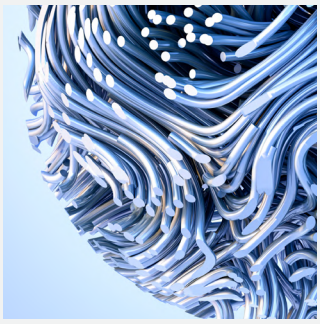
Construction organizations are poorly positioned to manage third party security risks with only **6%** reporting having adequate measures in place.

With the emergence of Industrial Internet of Things (IIoT) in the built environment and the digital transformation of construction operations, third-party security risks represent a material exposure to this historically less digitally advanced industry sector.

Accordingly, construction organizations need to adopt security assessments during third-party vetting and onboarding processes, and include cyber insurance provisions and vendor security remediation requirements in third-party contracts.

Concentrate on controls: **Ransomware**

59% of organizations have no formalized Business Continuity Management (BCM) process in place, and **69%** of respondents have no formalized incident response process. As the industry moves to a more digital environment, the potential for serious disruption is likely to increase.



Perfect the basics: **Regulation**

Construction organizations have been slow to adopt good practices concerning data security and regulatory management. Only **14%** of organizations report having adequate measures in place to manage their privacy and cyber security regulatory profile.

As construction projects adopt more data analytics and web-connected Operational Technology (OT), of Industrial Internet of Things (IIoT), and automation, regulations governing data privacy and security notifications will be increasingly important to their regulatory risk profile. Construction organizations need to get ahead of the curve with better governance and data protection measures.

Industry insights
Energy, utilities and natural resources

The role of energy in critical infrastructure and its financial clout, makes it an inviting target for foreign nation states, economic espionage, and hacktivists. Digital evolution, reliance on third-parties, and the rise of IoT smart devices and smart grids, make energy, utilities and natural resources organizations an attractive target.

How does the **energy, utilities and natural resources** industry stack up?

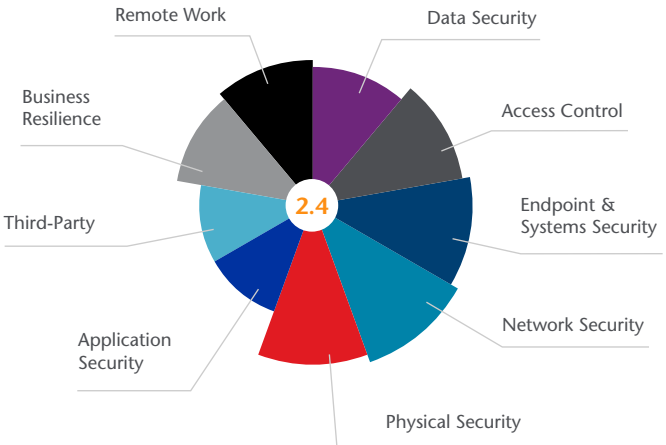
2.4 (basic)

The average CyQu rating for energy, utilities and natural resources organizations globally is 2.4/4 (basic).

What this means

This rating indicates that cyber security maturity is at a basic level. Organizational cyber security risk management practices and technologies are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. Risk management practices and technologies are not established organization-wide.

Explore the most pertinent cyber risks to energy, utilities and natural resources organizations, map them to key cyber security controls, and determine actions your organization can take to close cyber security gaps.



Security Domain	Industry Average	Global Average	
Rapid Digital Evolution			
Network Security	2.7	2.7	→
Application Security	1.9	1.9	→
Remote Work	2.4	2.5	↓
Third Party			
Physical Security	2.6	2.7	↓
Third-Party	1.9	2.0	↓
Ransomware			
Access Control	2.5	2.6	↓
Endpoint & Systems Security	2.6	2.6	→
Business Resilience	2.3	2.3	→
Regulations			
Data Security	2.3	2.4	↓

CyQu Scoring

Initial 1 - 1.9

Basic 2 - 2.5

Managed 2.6 - 3.4

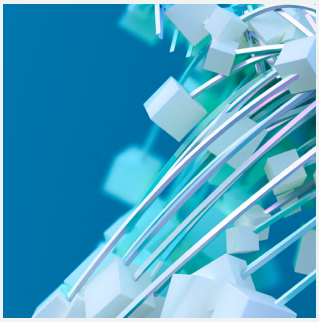
Advanced 3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu) is a cyber risk assessment that evaluates cyber risk across 9 security domains and 35 critical control areas.

Underpinned by proprietary data and expert insights, explore four key risk themes that are prominent to **energy, utilities and natural resources** organizations today.

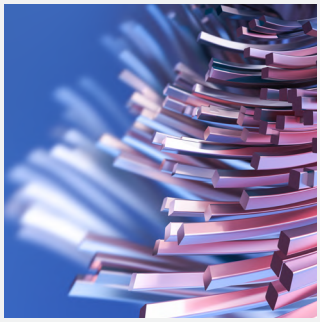
Navigate new exposures: **Rapid digital evolution**

There is a large discrepancy across organizations in this industry. While the majority are above the global benchmark, **24%** do not undertake any form of regular penetration testing. Conversely, **27%** employ best practices and regularly use external penetration testing teams to stress test control environments.



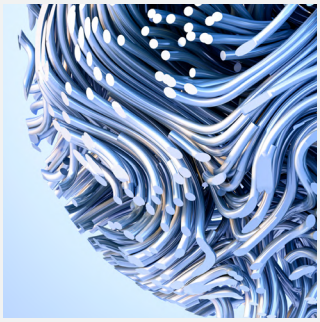
Know your partners: **Third-party risk**

This industry appears to have good basic third-party contract hygiene, with use of minimum insurance requirements and predefined Service Level Agreements (SLAs) for cyber security. That said, only **2%** of organizations obligate such controls for all contracts, indicating the importance of robust third-party assessment and layered controls.



Concentrate on controls: **Ransomware**

This industry is subject to a heightened number of incidents around data theft, espionage, and billing fraud. Taking this into account, it's not surprising that **21%** of organizations scored substantially higher than the global industry average for Incident Response (IR). However, **41%** indicated that they have an ad hoc approach to response.



Perfect the basics: **Regulation**

Embedding cyber risk management into wider risk management frameworks is a challenge for many organizations, with **61%** indicating they have not adopted the appropriate governance, risk management, or data protection measures. Collaboration with other risk management oversight functions such as, audit, Enterprise Risk Management (ERM) and legal, to measure and manage cyber risk, remains low. This impacts on an organization's ability to anticipate and respond to future privacy regulations.

Industry insights
Financial institutions

Under constant watch by regulators and the focus of data privacy laws, financial institution organizations are seasoned when it comes to navigating cyber risk. However, the shift to remote work means that many organizations are working hard to manage and mitigate unanticipated vulnerabilities.

How do **financial institutions** stack up?

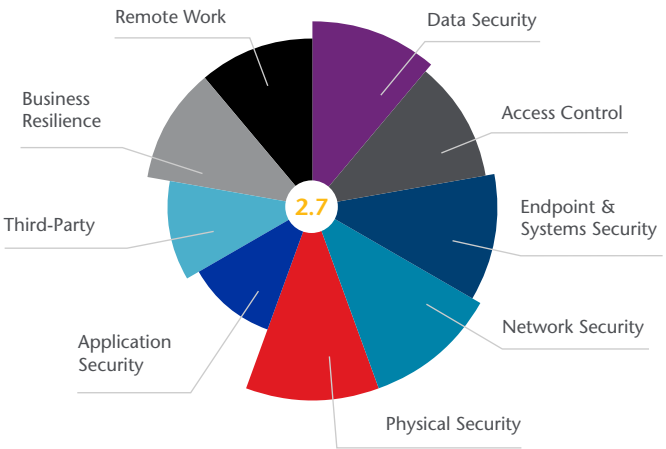
2.7 (managed)

The average CyQu rating for financial institutions globally is 2.7/4 (managed).

What this means

This rating indicates that cyber security maturity is at a managed level. Risk management practices and technologies are performed and established throughout the majority of the organization. The organization adapts its cyber security practices based on best practices and predictive indicators throughout the majority of the business. Policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk.

Explore the most pertinent cyber risks to financial institutions, map them to key cyber security controls, and determine actions your organization can take to close cyber security gaps.



Security Domain	Industry Average	Global Average	
Rapid Digital Evolution			
Network Security	3.0	2.7	↑
Application Security	2.2	1.9	↑
Remote Work	2.7	2.5	↑
Third Party			
Physical Security	3.0	2.7	↑
Third-Party	2.4	2.0	↑
Ransomware			
Access Control	2.8	2.6	↑
Endpoint & Systems Security	2.9	2.6	↑
Business Resilience	2.7	2.3	↑
Regulations			
Data Security	2.9	2.4	↑

CyQu Scoring

Initial 1 - 1.9

Basic 2 - 2.5

Managed 2.6 - 3.4

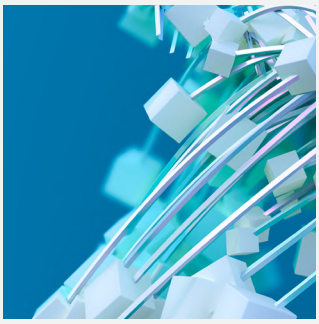
Advanced 3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu) is a cyber risk assessment that evaluates cyber risk across 9 security domains and 35 critical control areas.

Underpinned by proprietary data and expert insights, explore four key risk themes that are prominent to **financial institutions** today.

Navigate new exposures: **Rapid digital evolution**

The majority (**62%**) of financial institutions have mature network environments. This means that despite notoriously high volumes of legacy applications, there is robust architecture and strong defence mechanisms against perimeter breaches. There is also strong hygiene around network security, with **60%** conducting regular network penetration tests.

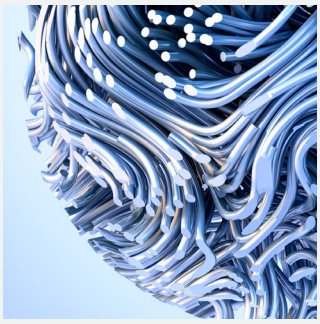


Know your partners: **Third-party risk**

Almost **2 in 5** financial institutions do not have a robust third-party due diligence process in place. In light of the recent high-profile events in the third-party space, this is a critical need for financial services.

Concentrate on controls: **Ransomware**

Almost half of organizations (**45%**), scan their attack surface for vulnerabilities. While almost a third (**27%**) have not implemented two-factor authentication across all remote logins.



Perfect the basics: **Regulation**

A reassuringly high number of organizations automatically encrypt data-at-rest, and in-transit. However, **18%** have not deployed an adequate data classification scheme. This highlights the challenge data-heavy organizations face in deploying a robust data management approach.

Industry insights
Life sciences

As a knowledge industry, life sciences is steeped in cyber risk. These organizations must secure sensitive client and patient information, and third-party risk is paramount as global partnerships are essential for the supply chain and to complete clinical trials. Add remote working to this, and the situation is challenging.

How does the **life sciences** industry stack up?

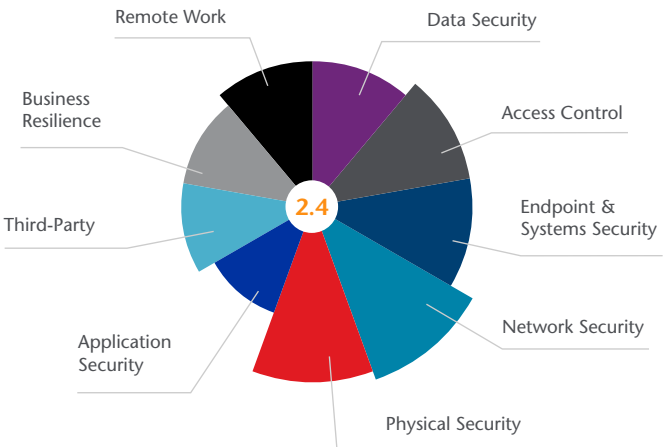
2.4 (basic)

The average CyQu rating for life sciences organizations globally is 2.4/4 (basic).

What this means

This rating indicates that cyber security maturity is at a basic level. Organizational cyber security risk management practices and technologies are not formalized. Risk is managed in an ad hoc and sometimes reactive manner. Risk management practices and technologies are not established.

Explore the most pertinent cyber risks to life sciences organizations, map them to key cyber security controls, and determine actions your organization can take to close cyber security gaps.



Security Domain	Industry Average	Global Average	
Rapid Digital Evolution			
Network Security	2.9	2.7	↑
Application Security	1.9	1.9	→
Remote Work	2.4	2.5	↓
Third Party			
Physical Security	2.8	2.7	↑
Third-Party	2.2	2.0	↑
Ransomware			
Access Control	2.6	2.6	→
Endpoint & Systems Security	2.6	2.6	→
Business Resilience	2.2	2.3	↓
Regulations			
Data Security	2.4	2.4	→

CyQu Scoring

Initial 1 - 1.9

Basic 2 - 2.5

Managed 2.6 - 3.4

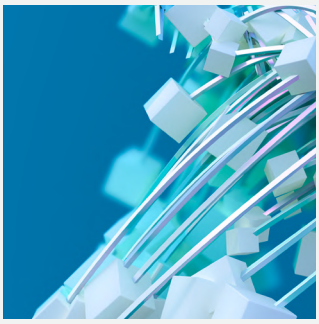
Advanced 3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu) is a cyber risk assessment that evaluates cyber risk across 9 security domains and 35 critical control areas.

Underpinned by proprietary data and expert insights, explore four key risk themes that are prominent to **life sciences** organizations today.

Navigate new exposures: **Rapid digital evolution**

For most life sciences organizations, a worst-case scenario is an attacker in the Operational Technology (OT) environment. Yet only **36%** of organizations report that they have regular penetration tests with both internal and external parties. Alarmingly, **17%** do not do any form of penetration testing. Specialist penetration testers are needed to help identify critical vulnerabilities.

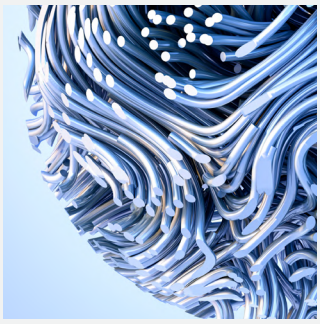


Know your partners: **Third-party risk**

Only **13%** of organizations have adequate 'third-party due diligence' assessments to prevent and detect third-party risks to confidential data, supply chain systems, and critical Operational Technology (OT) infrastructure. This exposes pharmacovigilance systems, distribution systems, and operational production processes to cyber attacks via third- party intrusion.

Concentrate on controls: **Ransomware**

Industry password management is taken very seriously, with **87%** of organizations adopting strong controls. However, only **17%** deploy strong Multi-Factor Authentication (MFA) across their Information Technology (IT) networks. This means password compromise can still lead to sensitive data compromise, or initial intruder access.



Perfect the basics: **Regulation**

As expected, this topic is a more secure area for life sciences given the highly regulated environment. However, the industry still lacks maturity, and data classification is a challenge. This is concerning given the data-heavy nature of the industry and the need to protect valuable intellectual property (IP). **37%** of organizations report not having an adequate approach to managing cyber security and privacy regulations.

Industry insights
Manufacturing

Manufacturing organizations do not have the same legacy experience as data-intensive industries, such as financial institutions. Today, manufacturing is seeing an acceleration in the pace of technological change evidenced by the digital global supply chain, connected devices such as Human Machine Interfaces (HMI), Industrial Control Systems (ICS), and the Industrial Internet of Things (IIoT).

How does the **manufacturing** industry stack up?

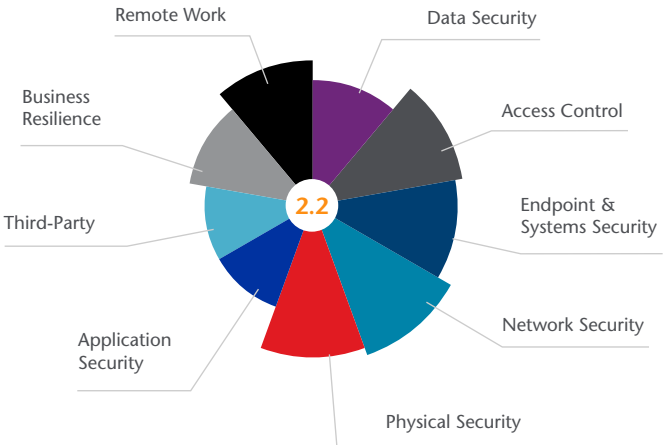
2.2 (basic)

The average CyQu rating for manufacturing organizations globally is 2.2/4 (basic).

What this means

This rating indicates that cyber security maturity is at a basic level. Organizational cyber security risk management practices and technologies are not formalized. Risk is managed in an ad hoc and sometimes reactive manner. Risk management practices and technologies are not established.

Explore the most pertinent cyber risks to manufacturing organizations, map them to key cyber security controls, and determine actions your organization can take to close cyber security gaps.



Security Domain	Industry Average	Global Average	
Rapid Digital Evolution			
Network Security	2.6	2.7	↓
Application Security	1.8	1.9	↓
Remote Work	2.4	2.5	↓
Third Party			
Physical Security	2.5	2.7	↓
Third-Party	1.8	2.0	↓
Ransomware			
Access Control	2.5	2.6	↓
Endpoint & Systems Security	2.4	2.6	↓
Business Resilience	2.1	2.3	↓
Regulations			
Data Security	2.1	2.4	↓

CyQu Scoring

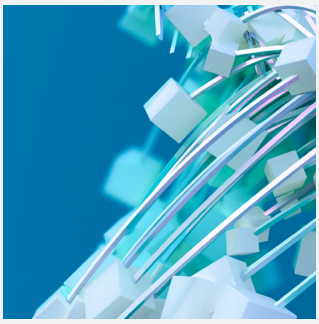
- Initial: 1 - 1.9
- Basic: 2 - 2.5
- Managed: 2.6 - 3.4
- Advanced: 3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu) is a cyber risk assessment that evaluates cyber risk across 9 security domains and 35 critical control areas.

Underpinned by proprietary data and expert insights, explore four key risk themes that are prominent to **manufacturing** organizations today.

Navigate new exposures: **Rapid digital evolution**

Unsurprisingly, clients in the manufacturing sector have a strong focus on environmental controls. For example, **37%** of all organizations have N+1 (parallel redundancy) configuration for critical power systems, fire suppression, and Uninterruptible Power Supply (UPS).



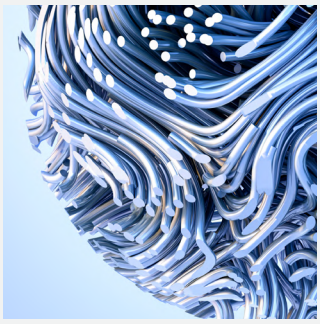
Know your partners: **Third-party risk**

Manufacturers are likely to depend upon a large number of third-parties to support their value chain. Yet more than half (**57%**) of organizations continue to perform ad hoc rollouts, without having formalized a consistent due diligence approach across their business. What is most concerning, is that **17%** have no third-party due diligence at all.

Concentrate on controls: **Ransomware**

60% of manufacturers do not implement Two-Factor Authentication (2FA), a critical additional security layer. Without authentication and encryption, **46%** of organizations struggle with endpoint logging and monitoring, causing poor visibility into Industrial Control Systems (ICS) and critical operational networks.

Most surprisingly of all, manufacturers still fall below the cross-industry average for both incident response and business continuity readiness.



Perfect the basics: **Regulation**

46% of manufacturers do not have a security solution that supports consistent and repeatable data classification. This also impacts their ability to layer additional data protection controls.

Industry insights
Professional services

Compared to many industries, professional services has weathered the COVID-19 pandemic relatively well. This is partly due to continued demand for its services, and also the ability for workers to shift to remote working with relative ease. This does not mean that cyber risk is irrelevant. The industry is a target for ransomware attacks, and firms report they are not managing cyber risk beyond the basic level.

How does the **professional services** industry stack up?

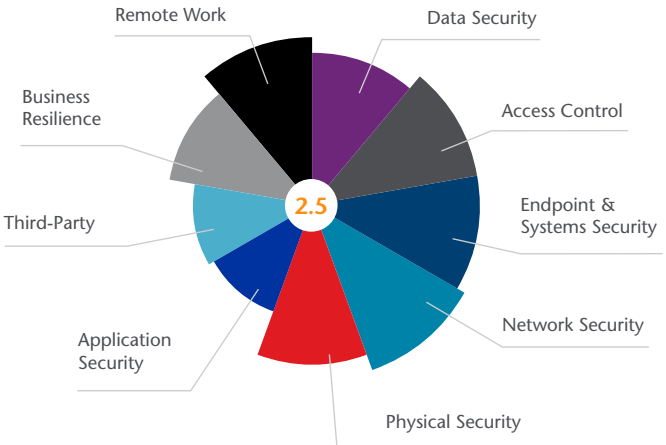
2.5 (basic)

The average CyQu rating for professional services organizations globally is 2.5/4 (basic).

What this means

This rating indicates that cyber security maturity is at a basic level. Organizational cyber security risk management practices and technologies are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. Risk management practices and technologies are not established organization-wide.

Explore the most pertinent cyber risks to professional services organizations, map them to key cyber security controls, and determine actions your organization can take to close cyber security gaps.



Security Domain	Industry Average	Global Average	
Rapid Digital Evolution			
Network Security	2.8	2.7	↑
Application Security	1.9	1.9	→
Remote Work	2.7	2.5	↑
Third Party			
Physical Security	2.6	2.7	↓
Third-Party	2.0	2.0	→
Ransomware			
Access Control	2.7	2.6	↑
Endpoint & Systems Security	2.7	2.6	↑
Business Resilience	2.4	2.3	↑
Regulations			
Data Security	2.5	2.4	↑

CyQu Scoring

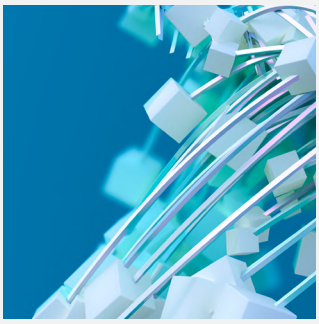
- Initial: 1 - 1.9
- Basic: 2 - 2.5
- Managed: 2.6 - 3.4
- Advanced: 3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu) is a cyber risk assessment that evaluates cyber risk across 9 security domains and 35 critical control areas.

Underpinned by proprietary data and expert insights, explore four key risk themes that are prominent to **professional services** organizations today.

Navigate new exposures: **Rapid digital evolution**

The management of device vulnerability in a remote setting has surfaced as a significant challenge in this industry, with **17%** of organizations having no formal approach or process. Alarmingly, only **4%** felt confident that they had a robust and consistent approach to this critical area.

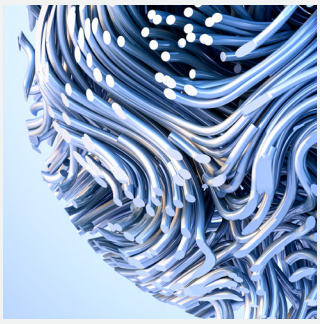


Know your partners: **Third-party risk**

Third-party management remains a real challenge, with **50%** of organizations presenting a risk maturity score of 1 overall. Of particular concern is the lack of attention to the due diligence of third-party providers, with **58%** of organizations lacking a formal process. As professional service organizations are often targeted because of the data they hold, this must be addressed.

Concentrate on controls: **Ransomware**

There is a big divide across organizations when it comes to ransomware security. **30%** have robust monitoring; leveraging next generation Endpoint Detection and Response (EDR) tools and behavioral analytics. Conversely, **39%** of organizations have very little monitoring in place. Without effective logs, it will be nearly impossible for these firms to confirm to clients whether their data may have been impacted by an attack.



Perfect the basics: **Regulation**

Risk management and governance of data remains an area of weakness for professional service firms. While **36%** had no real data governance processes in place, **45%** had no formalized approach to the risk management of data security. It is important that firms assess the financial consequences of a data breach on their organization.

Industry insights
Retail

Online everything was the theme for 2020, and retailers are continuing to see a demand for digital customer experiences. Already an industry fraught with cyber risk and under the watch of regulators, retailers now must identify and close the gaps resulting from rapid technology innovations, and continue to painstakingly protect sensitive customer data.

How does the **retail** industry stack up?

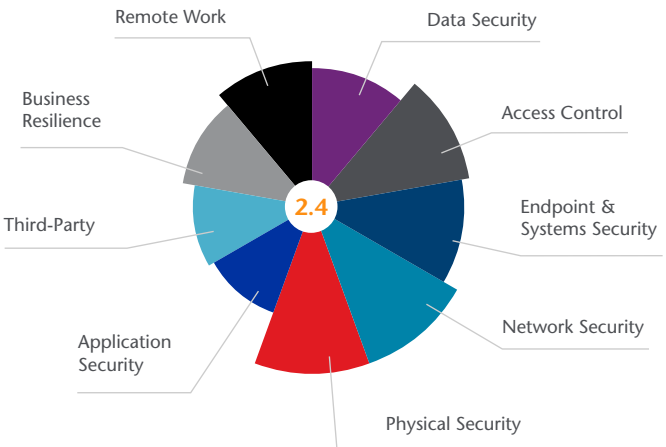
2.4 (basic)

The average CyQu rating for retail organizations globally is 2.4/4 (basic).

What this means

This rating indicates that cyber security maturity is at a basic level. Organizational cyber security risk management practices and technologies are not formalized. Risk is managed in an ad hoc and sometimes reactive manner. Risk management practices and technologies are not established.

Explore the most pertinent cyber risks to retail organizations, map them to key cyber security controls, and determine actions your organization can take to close cyber security gaps.



Security Domain	Industry Average	Global Average	
Rapid Digital Evolution			
Network Security	2.7	2.7	→
Application Security	1.9	1.9	→
Remote Work	2.4	2.5	↓
Third Party			
Physical Security	2.7	2.7	→
Third-Party	2.0	2.0	→
Ransomware			
Access Control	2.6	2.6	→
Endpoint & Systems Security	2.5	2.6	↓
Business Resilience	2.2	2.3	↓
Regulations			
Data Security	2.3	2.4	↓

CyQu Scoring

Initial 1 - 1.9

Basic 2 - 2.5

Managed 2.6 - 3.4

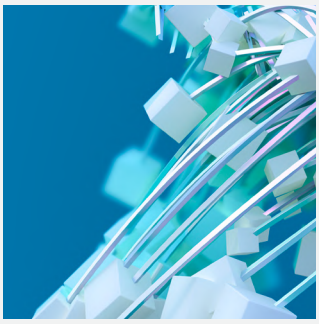
Advanced 3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu) is a cyber risk assessment that evaluates cyber risk across 9 security domains and 35 critical control areas.

Underpinned by proprietary data and expert insights, explore four key risk themes that are prominent to **retail** organizations today.

Navigate new exposures: **Rapid digital evolution**

There is a significant disparity in cyber risk maturity across organizations in this industry. **36%** of retailers indicate they are extremely vulnerable to network overload and Denial of Service (DoS) attacks. On the other end of the spectrum, **20%** of retailers reported advanced maturity, which suggests they have the ability to securely scale-up as consumer demand for digital channels continues to rise.



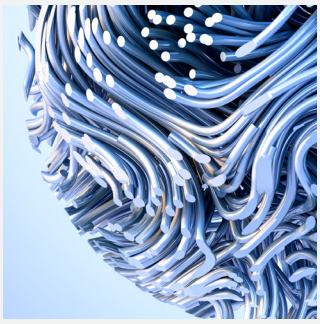
Know your partners: **Third-party risk**

More than half (**58%**) of retail organizations have inadequate third-party security measures, revealing the need for retailers to improve their ability to select and onboard third-parties.

While retailers excel in securing physical access to premises, stores, and offices, the testing of such security measures is weak. Physical penetration testing is not being implemented in a uniform way by **71%** of organizations. It is imperative that these physical measures are tested on a regular basis to maintain robust physical security controls.

Concentrate on controls: **Ransomware**

Given the increased number of ransomware-related attacks in recent months, it has become even more important to have effective business resilience measures in place. This is especially relevant in the retail industry, which has been increasingly moving sales and distribution processes online. Unfortunately, only **24%** of retail organizations have adopted adequate business continuity and disaster recovery measures for the increasing threat of ransomware attacks. As the success of retail organizations becomes more critically dependent on having readily available e-commerce and distribution systems, these organizations will need to address the poor state of their business resilience.



Perfect the basics: **Regulation**

With **40%** of organizations presenting a risk maturity score of less than 2, there is clearly improvement needed to ensure retailers are well-versed in managing and securing data. However, the fact that **30%** of organizations excel (risk maturity score above 3), suggests the industry is starting to approach a managed level of readiness.

Industry insights
Technology, media and telecommunications

Technology, media and telecommunications (TMT) organizations serve as an underpinning to all other industries, and demand for their products and services is more pronounced than ever. From electronic signature software, to 5G infrastructure implementation, and IoT, the industry is fundamental to the future of work. This is increasing the spotlight on cyber security, magnified by major recent events exposing vulnerabilities in global operating systems and supply chains.

How does the **technology, media and telecommunications** industry stack up?

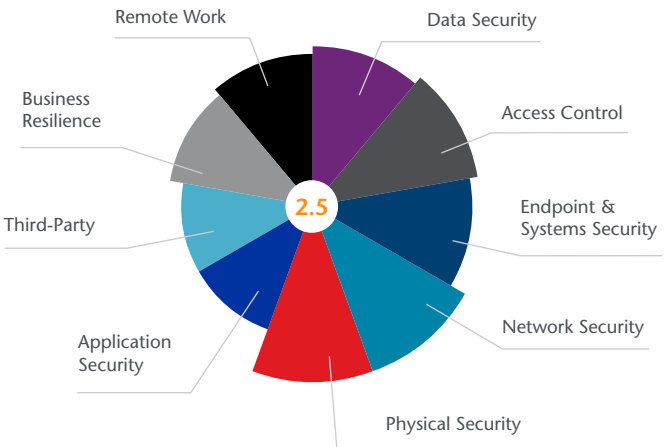
2.5 (basic)

The average CyQu rating for technology, media and telecommunications organizations globally is 2.5/4 (basic).

What this means

This rating indicates that cyber security maturity is at a basic level. Organizational cyber security risk management practices and technologies are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. Risk management practices and technologies are not established organization-wide.

Explore the most pertinent cyber risks to technology, media and telecommunications organizations, map them to key cyber security controls, and determine actions your organization can take to close cyber security gaps.



Security Domain	Industry Average	Global Average	
Rapid Digital Evolution			
Network Security	2.8	2.7	↑
Application Security	2.2	1.9	↑
Remote Work	2.5	2.5	→
Third Party			
Physical Security	2.8	2.7	↑
Third-Party	2.2	2.0	↑
Ransomware			
Access Control	2.7	2.6	↑
Endpoint & Systems Security	2.6	2.6	→
Business Resilience	2.4	2.3	↑
Regulations			
Data Security	2.6	2.4	↑

CyQu Scoring

Initial 1 - 1.9

Basic 2 - 2.5

Managed 2.6 - 3.4

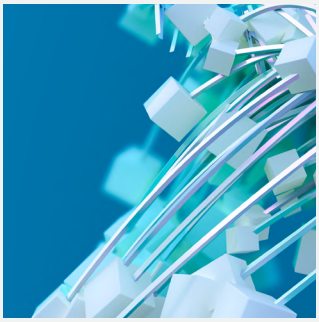
Advanced 3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu) is a cyber risk assessment that evaluates cyber risk across 9 security domains and 35 critical control areas.

Underpinned by proprietary data and expert insights, explore four key risk themes that are prominent to **technology, media and telecommunications** organizations today.

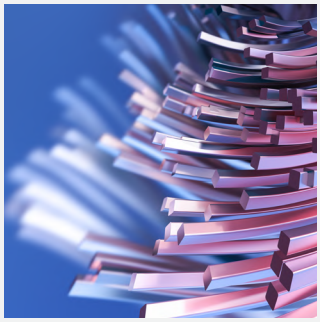
Navigate new exposures: **Rapid digital evolution**

It is surprising that **22%** of organizations do not use penetration testing, in any form, to contribute to the safeguarding of their environment. Given the intangible nature of technology, media and telecommunications asset classes, creating a resilient infrastructure is of increasing importance.



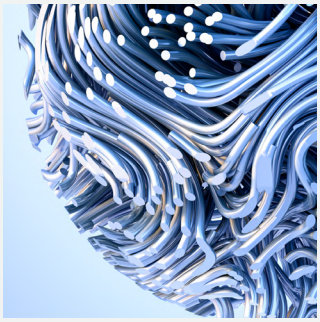
Know your partners: **Third-party risk**

Managing third-party risk highlighted a significant split in the industry, with **28%** of organizations indicating that cyber security is not specifically addressed when contracting with third-parties. Meanwhile **20%** of organizations indicate that cyber security is a critical component of all contracts, with explicit requirements and minimum standards built into contract wording.



Concentrate on controls: **Ransomware**

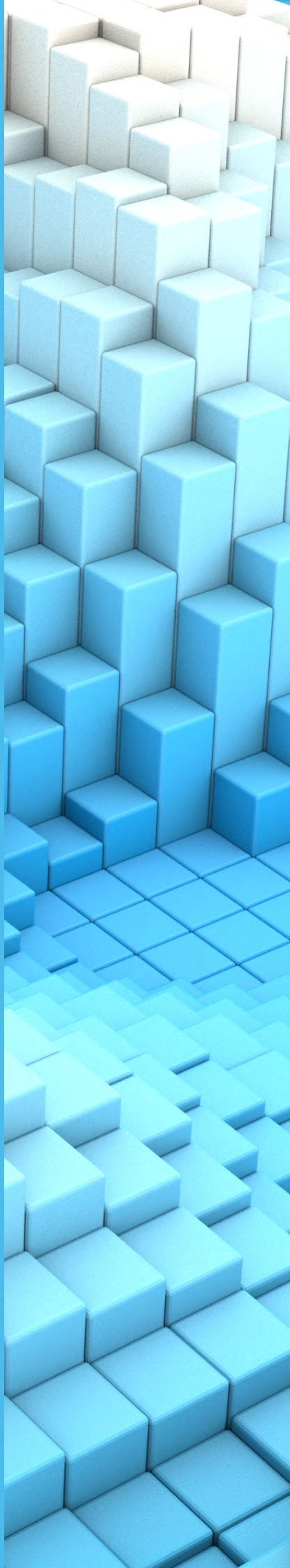
Endpoint security configuration has a real variance in responses. **37%** of organizations have very basic controls in place. However, on the opposite end of the scale, 31% of organizations utilize best-in-class methodology. Connected to this, **34%** of organizations do not monitor endpoints for suspicious activity – this is a challenge that must be addressed.



Perfect the basics: **Regulation**

User awareness training has been a big focus for this industry, with **46%** of organizations indicating that they employ a robust process including security training, regular phishing testing, and updates. However, **22%** of organizations struggled to deploy a robust and consistent approach to data classification, meaning that sensitive data may not have been identified and provided with the appropriate level of protection.

Conclusion



The opportunity

Predictions abound regarding the future of cyber risk. Instead of focusing on 'what's next?', this report has so far focused on 'what's now?'— in terms of what organizations should do to focus on risks today. To answer this, we relied on practical insight and hard data to explore the questions: What are the most pertinent cyber risks today, and how prepared are organizations across industries and regions, to manage these risks?

Now, we present the opportunities. Armed with knowledge, organizations have the ability to methodically ask the right questions to address cyber risk as an enterprise risk—to conduct a thorough assessment of cyber maturity and close the gaps that exist today.

Organizations also have an opportunity to become ready for tomorrow—to look to the future, and the changing cyber risk landscape. New risks are emerging daily and vigilance is essential.

Keeping the focus on today: making better decisions

The Cyber Quotient Evaluation (CyQu) data told us that organizations are performing under baseline when it comes to managing cyber risk. So, how do organizations become more prepared and protected?

Below is a blueprint to help organizations make better decisions by asking the right questions.

Assessment

- What is the state of our security and controls, in particular as they apply to digital evolution, third-party risk, ransomware, and regulatory risk?
- What are the most important assets we need to protect?
- What are the most likely threats?
- How do we balance business needs with cyber risks?

Quantification

- Do we know the type and materiality of our potential losses? For ransomware, do we know this beyond risk of data encryption?
- Do we understand key regulatory requirements and costs associated with non-compliance?
- How are we making security investment decisions?
- Can we measure the effectiveness of our current risk management and insurance, in terms of Total Cost of Risk (TCOR)?

Insurance

- Do we understand our exposures?
- Do we have an effective strategy to mitigate loss?
- Should we transfer a portion of our risk to the insurance market, or consider alternative risk transfer strategies?

Incident response readiness

- Do we have an appropriate, usable incident response plan? If yes, is the response team trained and ready to act?
- Do we have the right security and forensic tools, processes and procedures?
- Have we properly configured our cyber security technology?
- Can we quickly and effectively respond to an incident?

An eye on the horizon: be ready for tomorrow

Leaders from across Aon's Cyber Solutions singled out five notable risks that are critical in the near future. Being educated in these risks is essential.

- **Artificial Intelligence (AI)**. Machine learning is advancing at a staggering pace, and is an inevitable part of how organizations will do business. At some point, AI makes choices for us, and any choice that can be influenced or attacked poses a significant risk.
- **Alternative payments**. Wherever there is a transfer of funds, there is cyber risk. The developing world is in dire need of alternative payments, and new ways to accumulate and store wealth. Organizations will encounter counterparts who don't use banks, and business-to-consumer business models will eventually have nothing to do with traditional currency.
- **Retirement plans**. Retirement plans hold a wealth of data and are a gateway to vast sums of money. Organizations need to know who holds the keys to employee retirement data, and the fiduciary responsibility of the plan provider. As plans are increasingly accessed online and from mobile devices, this data is increasingly more susceptible to breach.
- **Technology supply chain**. Every year new exposures are introduced via technology providers. As more and more sensitive data and intellectual property is exchanged via third-party software, organizations must become vigilant in assessing vulnerabilities and exposure to cyber risk.
- **The Dark Web**. Fueled by the growth of cryptocurrency, the use of browser technology such as TOR, and the growing sophistication of ransomware groups, criminal markets are becoming stronger. The dark web is their workspace, and it is here to stay. Organizations should not try to navigate this space alone without a map or guide. Maintain constant vigilance.

Reference

1 "2021 Errors and Omissions and Cyber Insurance Snapshot: A focused view of 2021 risk and insurance challenges," Aon, https://www.aon.com/cyber-solutions/thinking/aons-errors-omission-cyber-insurance-snapshot-a-focused-view-of-2021-risk-insurance-challenges/.

2 "This Year in Ransomware Payments (2020 Edition)," December 2020. https://heimdalsecurity.com/blog/ransomware-payouts-of-2020/.

3 "2021 Errors and Omissions and Cyber Insurance Snapshot: A focused view of 2021 risk and omission-cyber-insurance-snapshot-a-focused-view-of-2021-risk-insurance-challenges/.

4 "Cyber Security Ventures," https://www.thesslstore.com/blog/ransomware-statistics/ https://www.sdxcentral.com/articles/news/ransomware-attacks-spike-148-amid-covid-19-scams/2020/04/.

5 "Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands," Coveware Ransomware Marketplace Report, Q4 2020, https://www.coveware.com/blog.

6 "Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands," Coveware Ransomware Marketplace Report, Q4 2020, https://www.coveware.com/blog.

7 "2021 Errors and Omissions and Cyber Insurance Snapshot: A focused view of 2021 risk and insurance challenges," Aon, https://www.aon.com/cyber-solutions/thinking/aons-errors-omission-cyber-insurance-snapshot-a-focused-view-of-2021-risk-insurance-challenges/.

8 "2021 Errors and Omissions and Cyber Insurance Snapshot: A focused view of 2021 risk and insurance challenges," Aon, https://www.aon.com/cyber-solutions/thinking/aons-errors-omission-cyber-insurance-snapshot-a-focused-view-of-2021-risk-insurance-challenges/.

CyQu risk maturity scoring

Initial | 1–1.9

Organizational cyber security risk management practices are not performed. If the organization identifies and addresses risks it is done within silos only; components and activities of the risk management process are limited in scope and implemented in an ad hoc manner.

Basic | 2–2.5

Organizational cyber security risk management practices and technologies are not formalized. Risk is managed in an ad hoc and sometimes reactive manner. Risk management practices and technologies are not established organization-wide.

Managed | 2.6–3.4

Risk management practices and technologies are performed and established throughout the majority of the organization. It adapts cyber security practices based on best practices and predictive indicators throughout the majority of the business. Policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk.

Advanced | 3.5–4

Adopts an organization-wide approach to manage cyber security risk. Organizational cyber security practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape. Process of continuous improvement incorporating advanced cyber security technologies and practices.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

For further information on our capabilities and to learn how we empower results for clients, please visit : http://aon.mediaroom.com

aon.com/cyber-solutions