The Cyber Arms Race
A retrospective on the last two years
by AnotherDay's global client cyber consulting team
2023
Introduction 03
About Gallagher 04
What this report is designed to do 06
About the Gallagher global cyber team 06
Priorities when engaging with insurers on cyber 08
What our consulting teams are seeing 14
Our 2023 watchlist: Systemic risk 22
Our 2023 watchlist: Other emerging themes 24
Contact 25
Introduction

The last 24 months in the wider cybersecurity ecosystem has been a whirlwind. The appearance of ever more insidious ransomware variants, a generational shift in working patterns, and unprecedented investment into technology and digitisation among large firms has shifted the balance of power between attacker and attacked.

In many cases, organisations have struggled to keep up with this new reality. Gallagher has worked with some of the largest organisations in the world to help them align their controls with their risk exposure. This report is the synthesis of that process and the lessons that we’ve learnt.

As with any major adversarial competition in human history, cybersecurity has become an ever-accelerating arms race to protect critical data, processes, intellectual property and reputation, and as a result the learning curves are relentless. The focus of conversations with Information Security and Risk Transfer teams have moved from deploying cloud security controls, to supply chain, to ‘beyond the network edge’, to ‘zero trust architectures’, and inevitably will move into even more novel areas over the next 24 months. In many cases, new initiatives are scoped and resourced before previous ones have come even remotely close to completion. This is the nature of an area of risk with malicious intent, where an adversary has as much choice about how the game plays out as you do. Chief Information Security Officers (CISOs) have been at the front line throughout.

It is this acceleration in the arms race which initially took the insurance markets by surprise. The explosion in ransomware losses just before and at the beginning of the pandemic revealed that many insurers had not been adequately assessing the exposure of their clients to cyber-related losses. We now use the term ‘silent cyber’ to describe how elements of insurance coverage for this esoteric risk were included in everything from property insurance policies, to kidnap and ransom response wordings. The industry had been talking about the perils of cyber for many years, with its aggregation and complex losses and impossible nature of attribution. Clearly, we learnt quickly that describing risks in the future was easier than proactively mitigating them.

In layman’s terms, organisations went from buying the digital equivalent of home and contents insurance, to trying to get hold of indemnification to protect them from hurricanes.

Many of our clients now spend much of their time dealing with the fallout of the collision between these two worlds. The rapidly changing cyber threat landscape has precipitated massive losses and extensive changes in how organisations protect themselves. These same losses have led to a doubling, tripling, or more of insurance premiums to allow insurers to build up reserves against potentially systemic exposures. This same cycle had occurred recently in the Directors’ & Officers’ insurance market, a cycle which took six years to come to fruition. In cyber, the cycle took six months. The role of cyber insurance also changed as a result. It went from being the type of attritional insurance policy that picks up small, regular losses to something resembling a ‘catastrophe class’. In layman’s terms, organisations went from buying the digital equivalent of home and contents insurance, to trying to get hold of indemnification to protect them from hurricanes. As any Caribbean insurance broker will tell you, the information requirements for the latter are very, very different from the former.

This painful process does, however, create significant opportunity for Information Security teams and for Risk Managers. The insurance market plays a very important, and usually unrecognised, role in holding risk management accountable.
and also has the ability to measure the return on investment of risk mitigation measures. If risk management is not working in a particular area, insurance losses explode. The subsequent increase in premiums increases the return on investment of mitigation and resilience projects as they become cheaper than buying insurance, subsequently decreasing losses and eventually premiums.

This tide ebbs and flows over time, becoming less pronounced as the data gets better and better. Tsunamis of change like the one we’ve experienced over the last two years in cyber become more like gentle waves as the insurance industry reacts to more pedestrian changes in the threat environment. A clear example of this process playing out elsewhere is Somali piracy which became a huge problem for shipping in the early 2010s. The advent of pirate groups targeting international shipping in the waters of the Red Sea and Gulf of Aden led to significant losses for insurers and increased premiums. These losses then precipitated requirements from said insurers to deploy armed teams on vessels, which brought attacks by pirates back down to a level close to zero: eventually this led to a decrease in premiums. The process led to a collapse in the cottage industry associated with piracy in Somalia, permanently affecting the threat environment.

At least, that’s how it should work. Broadly it functions well for natural catastrophes, political violence, and a range of other classes where data has been built up over decades and nasty surprises become less and less common (and, therefore, easier to cover by insurers). The trillion-dollar question is whether cyber is the outlier - does continuous technological change at exponential rates mean that data on attack vectors and losses becomes obsolete as soon as it’s modelled? If that is true, it means the cyber market will be in continuous flux regardless of how well insurers try to manage it through premiums, exclusions, and other tools. How will the market respond to quantum computing threatening the cryptographic protocols which underpin most methods of data encryption? What happens when a cloud infrastructure-as-a-service provider experiences a significant outage across availability zones? Only time will tell, but what is for sure, is that heightened information requirements and expectations for risk management will remain long after the threat of current ransomware variants has passed.

This brings us back to the opportunity for Information Security teams. For many years, information security conference slots have been taken up by talks with titles like “Demonstrating the value of Security”, “Measuring the return on Investment of Business Continuity”, or “Writing the Security business case”. A difficult cyber insurance market allows organisations an opportunity to try to measure the effect that their investments in security and resilience have, and it’s our job to try to help them do that. In this report we’ve outlined the type of measures best-in-class organisations are taking and how this aligns with the expectations of insurers, to help better align risk management and risk transfer for everyone. We hope you find it informative.

The AnotherDay cyber risk team
The Cyber Arms Race • A retrospective

What this report is designed to do

We wanted to provide large organisations (which we usually define as USD1bn+ in revenues, but this can be less) with a piece of evidence-based research which describes what we see our clients putting in place across a range of thematic areas and how these align to Insurer requirements for cyber coverage. We want to provide opportunities for Information Security and Insurance teams to sit down and discuss how these two areas have to connect, complement each other, and to create a benchmark which can be used to compare an organisation’s maturity with current practice for large clients.

The report is split into a number of sections, generally based on thematic risk control areas:

- **Network and perimeter security**
- **Endpoint protection**
- **Email and web security**
- **Access and account management**
- **Data protection & management**
- **Security monitoring and incident response**
- **Disaster recovery and crisis management**
- **Vulnerability and patch management**
- **Policy and governance**

Gallagher’s global cyber capabilities

Combined, Gallagher and AnotherDay’s global cyber capabilities comprises over 100 professionals positioned across threat intelligence, consulting, risk transfer design, (re)insurance broking, incident response and claims management. This expertise is multidisciplinary and provides a single approach for clients seeking to better understand their cyber exposures and align this to transferring this risk into the insurance markets. We have 24-hour capabilities and invest heavily in data and technology to take a scientific, evidence-based approach to advisory, particularly for very large clients who demand greater transparency and collaboration. We firmly believe that it is no longer possible to design appropriate coverage without having a comprehensive understanding of risk controls in place and how these are governed, assured and improved, coupled with help and advice to clients to ensure they are taking a ‘total cost of risk’ approach.
Priorities when preparing to engage with insurers on cyber
Priorities for engaging with insurers on cyber

Over the last two years, we have worked on over 50 cyber risk assessments in support of obtaining insurance coverage for large clients with over USD500m in revenues. These clients have come from a range of sectors, from manufacturing to telecommunications, pharmaceuticals to professional sports.

Working closely with our broking colleagues, we’ve learnt a lot of lessons in a relatively short period of time, with our approach tending to differ significantly when working with large organisations in comparison to those in the small- and mid-market space. Below, we outline five key priorities that we put into practice when engaging with our clients on cybersecurity.

Priority 1: Contextualising the role of risk transfer

This comes down to answering one question before even beginning an insurance placement process: why do we want to transfer some of our cyber risk into the insurance market? Organisations should be capable of clearly identifying their tolerance and appetite for cyber risk, and preferably should have educated the Board and senior leaders on the role of cyber insurance in the first place.

For instance, cyber insurance should be a mechanism for transferring residual financial risk off of the balance sheet (particularly in catastrophic scenarios) only once solid risk mitigation measures are deployed, as well as providing skill sets and response options which may be more difficult to engage individually (particularly network forensics, Incident response, and legal ‘breach coaching’). Everyone in the organisation, including Information Security, Risk, Insurance, the C-Suite and Board, should be on the same page about what cyber insurance is there to do and should be clear that it is only the final step in a process which should be rooted in Enterprise Risk Management (ERM) and risk assessment.

Making efforts to calculate potential losses from an adverse cyber event is also important here, as this would form the quantifiable basis of how much risk should be transferred to external markets in terms of limits and coverages. This alone has a number of considerations:

Consideration 1: What financial losses might be involved in a data loss or data exfiltration incident? Are these direct or indirect financial losses?

Consideration 2: What financial losses might be involved in a business interruption incident? Are these direct or indirect financial losses?

Consideration 3: How strong is our balance sheet to withstand that level of loss? Does it make financial sense to hold this risk on the balance sheet given tax, financial risk, operational risk, debt, and other liabilities and exposures?

Consideration 4: What might be the long-tail exposures of a badly-managed cyber incident based on previous case studies? What will the share price impacts be over the longer term for a publicly-traded company?

Consideration 5: What are other similar companies purchasing for the purposes of their cyber insurance limits, and why might that be relevant or irrelevant for us?

Consideration 6: Is there some way of quantifying the effectiveness of our cybersecurity control environment, and if so, what is the residual financial risk that would be left?
Priority 2: Establishing and bedding-in a cross-functional team

The biggest issue we tend to see in large organisations when advising them on their cyber risk is a siloed approach, particularly between Information Security, Information Technology, Insurance, Business Continuity, Legal and Finance. All of these stakeholders will have a role to play during the risk assessment and risk transfer process, for example:

- **Information Technology** provides information on how systems are architected, how networks and services are configured, and will usually be the first line of defence (‘1LOD’ in industry parlance) for implementing technical cyber measures such as patching;

- **Information Security** leads the charge on designing cyber security measures as part of a wider risk management strategy, and tracks and communicates progress on these initiatives to senior leadership;

- **Insurance** tends to take responsibility for managing brokers and advisers, question the involvement of particular insurance markets, assess the adequacy of insurance limits and coverages, and facilitates the interaction with Alternative Risk Transfer (ART) solutions such as captive insurers which are wholly owned by the organisation;

- **Business Continuity** teams provide information around the criticality of processes, how these interact with individual business models within the organisation, assess Critical Digital Assets (CDAs), and identify Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for individual systems and teams;

- **Legal** continuously manage the organisation’s liability exposures with clients and suppliers through contractual clauses, and develop and implement procedures and policies to respond to regulatory requirements (such as GDPR in Europe or HiPAA in the United States);

- **Finance** possess key data around how particular systems and processes drive revenue and profit, and therefore hold the key to understanding what the financial impacts of an adverse cyber event might be.

Putting this team together ‘in one room’ well ahead of engaging with insurers is critical, particularly if the organisation is conducting risk assessments to inform what residual risk will be transferred into markets. Personal relationships between these teams and knowledge of ‘ways of working’ when discussing cyber risk, can make all the difference in making an organisation fighting fit when preparing to talk about risk with external parties. This cross-functional team also can sometimes exist in other guises already, such as Cyber Security Working Groups or Information Security Executive Committees.
Priority 3: Understanding the business model/loss connection

Controls are important, but they’re not everything. An organisation’s business model (the way that it generates revenue and profit) and how it interacts with and depends on systems and processes at risk of a cyber event, plays a critical role in how impactful an adverse cyber event might be. We can describe a set of ‘layers’ which help to explain how this works:

Revenue generation relies on provision of products and services, which rely on processes, which rely on applications and tools, which rely on data and data transfer, which relies on infrastructure and architecture.

First, understanding these dependencies enables an organisation to map out what it needs to protect, allowing it to prioritise resources and activities in a way which supports its most critical processes that generate income. Second, as the nature of every organisation’s business model is different, companies can be inherently more resilient to cyber events than others, regardless of how mature their control environment is. Let’s take a worked example of this through the lens of two fictional companies:

**Organisation A** with USD400m in revenues has terrible controls from a cybersecurity perspective. Access management is rudimentary, security monitoring is non-existent, and architectural principles for setting up networking are not clearly defined. The organisation generates its revenues from the manufacture of premium, hand-made cigars predominantly in Central and South America which it mainly provides to wholesalers in large markets such as the United States, Europe, and Asia. Although the controls in this case are terrible, the nature of Organisation A’s business model (a handmade, premium product) means that there is little or no involvement of operational technology in the physical manufacture of their cigars: equally, their reliance on wholesalers rather than shipping to individual customers minimises the data that they hold. It also simplifies business continuity: if shipping systems go down, cigars can still be sent to wholesalers manually by making 40 phone calls instead of 600,000.

**Organisation B** with USD200m in revenues has impeccable controls including single sign-on across the enterprise which is supported by multi-factor authentication, a dedicated Information Security team, and rapidly maturing business continuity and disaster recovery plans which clearly identify the role of immutable backups. This organisation generates all of its revenues from the provision of a piece of Software-as-a-Service technology directly to large customers which sit under individually-negotiated contracts, as well as through an Application Programming Interface (API). This technology sits in single ‘stack’ of interconnected systems, meaning if one component or service fails the stack has a high risk of collapsing and preventing the provision of the product to customers. The technology stack also itself relies on external suppliers to function, such as cloud service providers, performance monitoring services, and integrations with other SaaS platforms. A major adverse cyber event, which will never have a zero likelihood of occurring regardless of how mature the control environment is, could generate huge losses both from data loss and business interruption.

Although this is just a thought experiment, it demonstrates that the nature of the business model has a significant effect on the exposure of a cyber event: the Potential Maximum Loss (PML) scenario for Organisation B will be much higher than Organisation A, despite the fact that the latter’s revenue is half that of the former. This relationship between the business model, underlying systems, and the cybersecurity control environment drives much of the conversation with insurers. It’s critical that large clients understand how this might differ across their organisation based on business unit.
Priority 4: Developing ‘transparent underwriting information’

The concept of ‘transparent underwriting information’ is difficult to define, but is also the foundation for any long-term risk transfer strategy for a large organisation. Importantly, it’s analogous to ‘transparent risk information’ within an organisation. Military and law enforcement regularly utilise the term ‘Common Recognised Information Picture’, which is, in essence, that all stakeholders are orienting themselves and taking decisions based on the same set of information which is as detailed as possible at any particular point in time. This ‘picture’ is what we aim to generate in collaboration with clients to share with insurance markets to connect risk management to risk transfer.

The two supporting pillars of this objective are ‘what the information is’ and ‘how the information is presented’. Both are as important as each other. The former generally relies on how comprehensive the information provided is relating to revenues, data, systems, and how these are protected across the organisation (see Priority 3), and then how granular this information is. Information which covers all business units in an organisation is comprehensive, and information which includes detail on individual lower-level systems is granular. Information provided to insurers for large organisations should be both, and it’s the role of the broker to advise on how this should work. These two are also not mutually exclusive. An information picture could be both comprehensive and granular, but equally may only be comprehensive (but not granular) or granular (but not comprehensive). If the information being discussed by the client, brokers, and underwriters meets both of these criteria then confidence and trust across all parties is significantly increased, which should improve the outcomes of the process.

Although it sounds superficial, ‘how the information is presented’ is equally important for a range of reasons, not least that underwriters are human and when dealing with a large number of potential client risks at any given time, will likely prioritise those in which the information presented is easy to absorb and digest. An organisation could provide reams of information which can be considered to be both comprehensive and granular, but if it isn’t accessible it becomes worthless. Returning to the military and law enforcement example, organisations in which the management of intelligence (read: information) is critical, huge investments have been made since 9/11 not just in the collection of data but also in how it’s presented to humans for analysis. Palantir, a Silicon Valley software giant, has been so successful partly based on its ability to make large amounts of information meaningful. It now has a market capitalisation of USD16 billion.

Client risk management and insurance teams, alongside the partner broker and advisors, have the greatest success when executing a strategy which develops a Common Recognised Information Picture which is comprehensive, granular, accessible and digestible. This ‘transparent underwriting information’ then serves to increase the trust and confidence of insurers, particularly when it’s fully contextualized. It also serves to reinforce that disclosure requirements were fully met at placement when negotiating over any subsequent claim. As many underwriters have quietly explained, “we don’t trust anything now which looks perfect.”
Priority 5: Setting expectations on timeframes

The last area that we’ve found to be a common area of frustration is the time now associated with the renewal of a cyber policy for a large organization. Partially, this is likely the result of an extremely rapid transition between a state of play where a policy would take a Risk Manager hours to procure to the current state where the process will take months (and probably tens of person hours of time, or more). This frustration will likely dissipate as heightened information collection requirements become the new normal, but in the interim, convincing disparate teams across an organisation to become involved in the information discovery and renewal process can be difficult.

There are a few ways to deal with this. We tend to find that the best way to set expectations is to characterise the process as part of governance and enterprise risk management generating an outcome which is relevant and actionable to the organisation, unconnected with insurance. The transfer of this risk financially into the market is just a byproduct of the process rather than its aim. Once stakeholders understand that this forms part of enterprise risk management, rather than teams ‘doing a favour’ to the Insurance team, the dynamic changes and additional time and resource tends to get prescribed. A consulting-led approach here can underline this very clearly.
On-the-ground, and out in the ether: what controls & issues we’re seeing across large clients
What our consulting teams are seeing

We want to share the insights of our global consulting team from working with large clients as to where their risk management controls and practices tend to align with market expectations of ‘minimum standards’, or not. Like it or not, insurer requirements will likely increasingly be seen as another critical standard for large organisations to work to.

Internationally recognized frameworks such as NIST, ISO 27001 or CIS are effective, however the insurance industry’s requirements represent a near-real time snapshot of what is working – and what isn’t – using information from hundreds of claims globally. We’ve broken our findings down into two areas: what we are seeing from clients, and the expectations of markets over the last two years. We hope this will provide some useful insight into how risk management can be closer linked with risk transfer.

Network and perimeter security

The last two years has seen a significant hardening of the market around network and perimeter security controls, likely stemming from the global ransomware epidemic that has dogged the information security community increasingly since 2019. Since the Covid-19 pandemic and resulting shift to more hybrid forms of work, we’ve seen requirements tighten around the configuration and use of Virtual Private Network (VPN) and Remote Desktop Protocol (RDP) network connections.

Both are now commonly exploited by ransomware hackers, with insecure configurations providing attackers with easy initial access to a given network. As a result, we’re now seeing underwriters demand that MFA is deployed for all remote access, with access to the network only provisioned through the use of a VPN. Where RDP connections are required, however, not only are we seeing MFA stipulated as an absolute minimum requirement, but we’re also seeing a market shift that questions its necessity entirely given its susceptibility to ransomware.

Despite these notable market shifts, it is also the case that network and perimeter security are one of the strongest areas for our clients – whether that’s through strong network segmentation, firewall configuration (including for web application firewalls – or WAFs), and the use of intrusion detection and prevention systems. When working with clients across various sectors, we’re noticing greater care and attention being paid to the way in which different areas of their network are being segmented (between, say, an enterprise network and local network at a manufacturing site) and the controls being deployed to inhibit an attackers ability to move laterally throughout a network. For large clients we’re yet to see widespread implementation of zero trust architectures. That being said, our market-led assessments are still picking up a number of regular red flags, particularly around the use of interactive logins to servers for service accounts, and firewalls allowing RDP connections by default, rather than by exception.
Endpoint protection

Unsurprisingly, the insurance markets have remained fairly resolute in stipulating that clients must, as a minimum security requirement, have an Endpoint Protection and Response (EDR) tool deployed across their network (preferably covering 100% of all endpoints and servers, unless compensating controls are utilised). As phishing remains one of the most prevalent attack vectors for threat actors to gain access to a network, an EDR tool is considered a crucial facet (among many others) in bolstering an organisation’s security posture, providing effective detection and response capabilities on all endpoints for containing malware in the event of a compromise. Nearly all clients we work with have demonstrated a strong security posture when it comes to protecting end user devices and servers, through EDR deployment, full volume encryption and host-based firewalls across their entire network or on end user systems such as laptops and workstations.

One area of concern, however, is that we are seeing clients not extending this protection to mobile devices and allowing employees to ‘bring their own devices’ (BYOD) to work and sometimes onto the company network. Without the same level of protection, appropriate segregation and a lack of clear policy, BYOD risk remains an obvious blind spot, potentially opening the gap to significant data loss or insider attacks. Related to this risk exposure, underwriters are also showing a greater interest in asset management processes, and whether client’s are maintaining a current and up-to-date inventory of all enterprise hardware and software assets with managed configurations.
Web and email security

Across the board, our clients continue to show a really healthy position on all things web and email security. For the most part, we believe this is likely a result of a pandemic-induced shift to remote working and the growing number of opportunities this presented to threat actors to target companies through coordinated phishing campaigns and web-based malware. In response, the security vendor market has also seen increased competition, leading to a greater selection of web and email security solutions (e.g. Fortinet, Defender, Proofpoint, Mimecast, Barracuda) that provide advanced protection through various gateways, protocols and filters. On top of this, we’re seeing nearly all of our clients implementing regular (at least semi-annual) phishing exercises across their organisation, with the process outsourced to a growing market of third-party providers (e.g. KnowBe4, TitanHQ, Cybsafe, Proofpoint).

Amongst more advanced clients, we’ve increasingly seen the adoption of Secure Access Service Edge (SASE) technologies such as Zscaler and Cisco Umbrella. Combining software-defined wide-area networking (SD-WAN) and VPN capabilities with various cloud-based security functions (e.g. secure web gateways, firewalls and zero-trust network access), we’re likely to see SASE technologies replace traditional VPN access as large organisations move more and more towards cloud-based architectures, largely due to their scalability and zero-trust principles. That said, there still appears to be little understanding amongst underwriters as to the functionality of SASE technologies, which can create challenges when attempting to demonstrate why these have replaced controls more familiar to markets, such as VPNs. This is one small example of why it is so important for clients to provide comprehensive, granular, accessible and digestible underwriting information that goes beyond the traditional proposal form.

Vulnerability and patch management

Comprehensive vulnerability and patch management processes are yet another key indicator of an organisation’s cybersecurity posture and maturity. In response to a number of zero-day exploits that have plagued the information security community over the last 2–3 years (e.g. SolarWinds, Kaseya, Microsoft Exchange and Log4j), market requirements have hardened significantly in this area. For example, a critical minimum security standard for underwriters stipulates that clients should have a documented and audited patch management strategy, setting clear policies regarding patching cadence, ensuring that metrics are reported correctly, and that the correct amount of resources are in place to deliver against them.

We’re also seeing the markets change around vulnerability management, with clients now expected to perform regular vulnerability risk assessments and penetration testing against both internal and external facing environments. Despite these shifting requirements, we’ve noticed that vulnerability and patch management are arguably the most immature (and challenging) areas from a controls perspective, with clients often having limited vulnerability scanning capabilities (for example, not covering 100% of their network), limited patch processes, or a mixture of the two. Because of this, this is an area we are regularly emphasising to clients as an area in need of attention and resource.
Access management

Access management has become one of the fastest moving – and hardening – areas of the market over the last 2-3 years, with requirements around multi-factor authentication (MFA) and privilege access management continuing to get more robust. For example, MFA is now a critical minimum security requirement for underwriters across areas of employee email access (incl. on personal devices), remote access (e.g. VPN, RDP) and privileged access management. Against this backdrop, it is of no surprise that clients are often found playing catchup, whether this is through the deployment of MFA and Privileged Access Management (PAM) tools, or through the implementation of stringent privileged access management policies. For our largest clients, we see that MFA has been comprehensively implemented for remote access, however we’re seeing that privileged accounts are left more exposed. Despite this, most clients have plans in place for rolling out additional authentication, particularly for their most critical accounts such as domain administrators.

On top of growing MFA requirements, we’re also now seeing underwriters focus specifically on granular levels of access control management for local admins and privileged and service accounts. Underwriters are also showing greater concern around access and footprint of domain accounts across an organisation’s network. Because of this, clients are now expected to invest and integrate a PAM tool as a crucial facet of their access control processes, with the vast majority of large clients now adopting ongoing programmes to roll their privileged accounts into a PAM tool. However, a number of (typically agile, cloud-native) organisations are now shifting to an Identify and Access Management (IAM) model, allowing them to bring many forms of authentication together based on user attributes and provides role-based access control across the organisation.

Without appropriate Privileged Access Management, even simple ‘credential stuffing’ attacks as the one above can quickly result in adversary lateral movement.
Data protection and management

The last 24 months has seen a rapid hardening of the market across areas of data protection and security, with underwriters not only pushing for more stringent data classification and management policies, but also ensuring that clients are investing in the right kind of security tools and processes that protect data across their networks. On top of investing in various data encryption technologies and password management tools at an end user level, we’re also seeing clients invest in Data Loss Prevention (DLP) tools at a network level in order to detect and prevent data breaches across the organisation. For some of our larger clients, however, the complexity of configuring DLP across their entire network has proved to be an enormous challenge for security teams, naturally leading to a slower (and sometimes costly) roll out.

Against the backdrop of increasingly more stringent data protection and data sovereignty laws for our clients around the world (e.g. GDPR, NYPA, LGPD), we’re also seeing underwriters show a greater interest in how data protection policies are managed and implemented: for example, how records are stored, managed and reviewed, and whether such policies comply with local data protection laws and regulations when data is exported or stored in different jurisdictions globally. With more clients collecting and retaining various forms of biometric data, underwriters are now also requesting greater clarity on how such data is handled, stored and retained.

Policy and governance

Security governance is yet another crucial component of an organisation’s cybersecurity maturity and posture, effectively allowing them to control, direct and communicate their cyber risk management activities and overarching approach to security. Nearly all clients we work with have a mature and robust information security governance and management structure, including well developed policies and compliance with internationally recognised standards, and an effective programme of cybersecurity education and awareness training. It is now a standard minimum requirement from underwriters that clients have implemented cybersecurity awareness training for employees on at least an annual basis, with the vast majority now doing so through a number of trusted third-party vendors (e.g. KnowBe4, CybSafe, Proofpoint, Mimecast).

With the enduring threat of phishing and business email compromise (BEC) attacks against organisations, underwriters are also focussing in on the type of training is conducted, such as the inclusion of data handling, how to recognise social media threats, and more targeted training for those employees handling more sensitive data in high risk roles such as HR or finance. Compliance on these more granular processes is patchy however, which may speak to a disconnect between the cybersecurity awareness vendor community and the kinds of breaches and claims underwriters are seeing on the ground.

The last 12 months has also seen a growing risk emerge with regards to employee activity on company devices (e.g. accessing personal emails or social media) and how this is leading to more security incidents. As a result, the insurance market is now taking a greater interest in our clients’ Acceptable Use (AUP) and clear desk policies, and how non-compliance may be creating greater exposure to phishing and social engineering attacks.
Security monitoring and incident response

In order to improve a client’s ability to monitor, detect, investigate and respond to an incident, investments in security monitoring capabilities and tools (such as a SOC and SIEM tool) are seen as critical components to an organisation's overarching security posture and its ability to respond to an ever-changing cyber threat landscape. Accordingly, insurance market applications now drill down into specific components of an organisation’s security monitoring capabilities, from the active logging and monitoring of unusual activity on their network, to the extent to which their SIEM tool leverages automation to improve the time to detect and triage significant events (for example: alerting the SOC in the event of unauthorized remote access to a critical system or service). In the last year, due to an increase in attacks targeting weaker security controls in Active Directory (AD) and its importance to threat actors seeking to escalate their privilege, underwriters have also centred their concerns around whether clients are regularly auditing and actively monitoring their AD for signs of compromise.

The vast majority of clients we work with have excellent 24/7 security monitoring capabilities, either through an internally or externally managed SOC (e.g. Secureworks, Trustwave, Mandiant) and augmented by a third party SIEM tool (e.g. Rapid7, Salesforce, Datadog). Typically, our larger clients will operate a tiered SOC structure in order to enhance their detection and response capabilities, whilst a number of clients are now adopting a hybrid SOC model, which allows for greater collaboration between internal security teams and third-party security experts. Despite notable progress in this area, a large number of clients with OT exposures are still being slow in terms of integrating their OT environment into their SOC capability, creating a significant blind spot in areas of the network that are often critical to revenue generation.

Beyond the SOC and an organisation’s security monitoring capabilities, underwriters are also showing a greater interest in how organisations respond in the event of a cyber incident. Traditionally, we’ve seen the development and documentation of a Incident Response Plan (IRP) as a useful yardstick for understanding a client’s cybersecurity resilience and posture. But increasingly this is changing, with markets now showing more of an interest in how regularly such plans are exercised and whether they incorporate external stakeholders. Whilst nearly all of the clients we work with have a well developed IRP in place, with clearly defined roles, communication lines and training, we are also seeing notable gaps in testing frequencies and IRPs not including critical third-party service providers or playbooks for responding to ransomware, web application incidents and denial-of-service attacks.

We continue to hear large clients talk about the ‘single pane of glass’ objective for analytical security and logging information united by a SIEM solution, with EDR and ActiveDirectory continuing to be the main data sources. Some clients are also moving to cloud SIEM deployments.
Disaster recovery and crisis management

Backup and disaster recovery processes are now seen as critical functions within any modern-day organisation. Not only do they play a vital role in reducing the damage or disruption that could be caused by an incident or disaster, but can also dictate how quickly an organisation can recover to an operational footing. Such processes are therefore intrinsically linked to the overarching stability of an organisation, with poor backups and disaster recovery processes leading to potential enormous operational and financial costs in the event of a disaster or cyber incident such as a data breach or ransomware attack.

Against the backdrop of the recent ransomware epidemic globally, it is of no surprise that requirements around business continuity (BC) and disaster recovery (DR) processes have strengthened significantly. For example, clients are not only expected to develop and implement rigorous BC and DR plans that cover IT/cyber emergency scenarios across all facets of the organisation, but underwriters are also increasingly interested in how such plans are reviewed and maintained, and how often backups and critical systems are tested and restored. Underwriters are now also seeking much more granular information from our clients, from how and where backups should be made (including backup frequencies and recovery times for critical systems) to stipulating that critical data and systems should now, at a minimum, be backed up off-site (preferably offline, for example on disk, tape or an isolated cloud environment). Understandably, BC and DR processes differ from client to client, but we are seeing a steady maturing in this area as organisations begin to marry both as part of wider organisational resilience. For our largest clients, we’re seeing a notable drive towards migrating backups into cloud environments, often air gapped from the main network, as part of their backup strategy (utilising third-party vendors such as AWS and Azure), whilst a growing number of technology-oriented service providers we work with appear to be making the shift towards an agile, cloud-based architecture in order to increase resilience and reduce operational and security overheads.

Due to the increasing threat of ransomware, we’ve also seen the insurance market grow increasingly concerned with the crisis management capabilities of our clients, with market applications now attentive to how regularly clients conduct cyber exercises and scenario planning. Worryingly, this is a real area of oversight with clients still, with cyber exercises still incredibly nascent and lacking any coverage around ransomware and how they should respond in the event of a customer of third-party vendor being impacted.
Our 2023 watchlist: emerging themes
The Cyber Arms Race • A retrospective

Our 2023 watchlist

Top of the list: Emerging concerns around ‘systemic’ risk

Cyberspace is exceedingly and increasingly complex, containing millions of interdependencies, and a huge challenge for the cyber insurance market is understanding and quantifying the risk of a ‘systemic’ event that impacts a huge proportion of their client base at once. This type of event is classed as a ‘systemic risk’ and, in the cyber domain, usually results from the existence of a single point of failure in a key piece of software used across businesses, governments and society that could cause a major national or global impact. Impact can appear in many ways, for example a cyber-attack on one of the world’s largest cloud service providers would have broad financial, social, and political effects, and could create insurmountable costs for the cyber insurance and reinsurance industry.

The industry has faced incidents that point to a degree of systemic risk. For example, Log4j, a piece of software embedded across millions of consumer devices, contained a significant vulnerability that prompted investment from businesses globally to rapidly patch their systems. SolarWinds is another example of a serious vulnerability that crossed national boundaries and resulted in sensitive data being released from governments and core technology providers such as Microsoft. From an economic and social point of view, there are few examples of a more damaging systemic cyber risk than that posed by WannaCry and NotPetya, which exploited the lack of investment in updating IT infrastructure and appropriate risk management. WannaCry, whilst global in Impact, managed to take vital healthcare services offline in the UK’s NHS and cost millions in remediation. NotPetya, on the other hand, cost global businesses, including Maersk and Merck, an estimated USD10 billion in total to restore their operations.

For businesses, as cyber supply chains grow, it is increasingly critical that there is a clear understanding of the risks posed by ‘one to many’ service providers, who often give rise to systemic risk events. Below we provide some guidance, based upon best practices and our experiences with large clients, that can help to ensure organisations can accurately assess and manage their exposure to systemic risks.

Define security requirements linked to the criticality of the service: As a first step, it is important to understand how critical the supplier’s offering will be to your business. Usually this can be assessed using a business impact analysis or interrogating what impact disruption to the service offering could have based on an internal risk matrix. The higher the criticality, the more focus there should be on security requirements and the lower your risk appetite should be.

Ensure the supplier completes a security questionnaire based upon an internationally recognised standard: Most suppliers will be able to provide information on their compliance to ISO 27001, the NIST framework or CIS controls, however it’s important that you push to get information on the types of controls in place at the supplier, to satisfy yourself that they meet your standards. This is not always possible, particularly with ‘one to many’ suppliers such as AWS, Oracle etc, so instead it is important that you receive evidence of accreditation to a security framework. Some suggested control question requirements are provided below as a minimum standard for critical suppliers:

- MFA for all employee email
- MFA for remote access
- Privileged Access Management w/MFA
- Offsite (preferably offline) backups
- Hosting config that meets your RTO/RPO
- Utilise EDR on all managed endpoints
- Have a 24/7 SOC with associated SIEM tooling
- Acceptable cadences for patch management
- Continuous vulnerability scanning
- Mandatory cybersecurity e-Learning
Strong email and web filtering tools
- Privileged account controls for admins
- Credential rotation and vaulting
- Regularly exercised disaster recovery plans

Web application firewalls
- International security standard accreditation
- Logical isolation of your instance from others

Where suppliers cannot meet your security standards, this should be raised as a risk, so that it can be appropriately quantified and internal mitigating controls put in place: It may not be possible for a preferred supplier to satisfy all of your security requirements, however being able to identify these gaps as discrete risks allows them to be appropriately quantified, and internal controls put in place to reduce your exposure.

Ensure you have contractual obligations in place regarding information security: Although most contracts include a data schedule (to ensure suppliers meet GDPR requirements), many companies still do not draft stand-alone information security schedules. This provides some contractual recourse in the event of a third-party breach and also enables some level of assurance through the ability to require evidence of security controls on a recurring basis. As a minimum, this schedule should include:

- Service level agreements for incident notification, response and engagement with you during an incident.
- A clause that stipulates any resilience requirements for the service (IE recovery time and recovery point objectives in the event of disaster), availability (uptime), and SLAs for monitoring service levels.
- A clause stipulating that the service provider must adhere to an internationally recognised security standard, and be prepared to provide evidence of such certifications on an annual basis for assurance.
- A regular cadence of security-focused supplier performance meetings (or a standing agenda item for the supplier to report against security requirements during broader supplier performance meetings).
- Escalations and penalties in the event that the service provider is in breach of this schedule.
- Bear in mind that larger suppliers are unlikely to take your schedule wording verbatim (or at all) and some negotiation may be required.

As you onboard more service providers, maintain a view of risk aggregation across cloud services, including specific data regions within each provider: The vast majority of Software-as-a-Service providers utilise AWS, Microsoft Azure or Google Cloud Platform to host their applications. As your cloud supplier footprint increases, it is important that you understand your risk aggregation across these suppliers. As part of onboarding, you should ensure that you know which cloud service provider the supplier relies on, and the availability zones and data regions that they are hosted in. This will support decision making regarding systemic risk (ie. a major outage of AWS in Europe due to energy black outs for example), and ensure you can maintain resilience by diversifying your supplier base through visibility of their critical 3rd parties (your 4th parties).
Runners-up: Other themes to watch

We're watching closely the progress of the Russian invasion of Ukraine as the dynamics of the conflict in that theatre can have outsized effects on the tactics, techniques and procedures of ransomware (and other) threat actors. Cyber methods can be used offensively and defensively by both sides in a way which is non-attributable, meaning that the likelihood of attacks being carried out against international targets is heightened. On the opposite side of the coin the grinding war has meant that mobilisation in both countries has significantly depleted the pool of talent used by threat actors - recent communications leaks from the Russian threat group Conti corroborate that this is having an effect on operational capability. As it stands, it's unclear which dynamic will have a greater impact on our client base in 2023.

The volatile fortunes of web3.0, and cryptocurrencies in particular, are also likely to have an impact on the types of attacks that will affect large clients in the coming year. This volatility is the equivalent of ‘foreign exchange’ risk for threat groups which demand ransoms in cryptocurrencies such as bitcoin, and the more this market fluctuates the greater the impetus for them to diversify into other areas. We've seen a marked uptick in Business Email Compromise losses where traditional fiat currency is diverted into a third bank account as a result of a spear phishing attack against a finance team or member of senior leadership: as the payment is often in US dollars (or some other stable, real-world currency) this crypto risk is significantly reduced. We are also closely watching whether there is likely to be an increase in ransom payments through privacy coins such as Monero, which are significantly harder to trace.

The advent of ChatGPT has generated concerns for us around the weaponisation of Artificial Intelligence. Although this is likely a longer term trend, the technology from OpenAI has demonstrated that this kind of chatbot – which would be classed as ‘narrow AI’, as it performs very specific functions and has no general sentience - can still be realistic and conversational enough to pass the Turing Test and fool a human into thinking it's having a conversation with a real person. If this kind of technology was weaponised by threat groups, it could rapidly complicate attempts to train users on spotting and reporting (spear-)phishing attempts. Could your colleagues spot a potential Business Email Compromise attack if they had exchanged nine emails with an attacker who spoke perfect English, and had access to everything which was publicly known about your organisation?

The continuation of the move by more mature clients to ‘zero trust’ models will test the assessment questions and approaches of major insurance markets. Micro-segmentation at this level can be extremely difficult to explain and communicate, particularly in organisations where this is deployed in some areas and not others. The ability to eloquently describe and evidence a zero trust architecture could unlock significant premium and coverage advantages in the longer term with underwriters who understand and embrace its benefits, but could butt up against a very established question set which is geared towards more traditional infrastructural models.
Contacts

Jake Hernandez
CEO, AnotherDay
Phone: +44 7599 897412
jake.hernandez@another-day.com

Adam Carrier
Head of Consulting, AnotherDay
Phone: +44 7979 404444
adam.carrier@another-day.com

CONDITIONS AND LIMITATIONS

This information is not intended to constitute any form of opinion or specific guidance and recipients should not infer any opinion or specific guidance from its content. Recipients should not rely exclusively on the information contained in the bulletin and should make decisions based on a full consideration of all available information. We make no warranties, express or implied, as to the accuracy, reliability or correctness of the information provided. We and our officers, employees or agents shall not be responsible for any loss whatsoever arising from the recipient’s reliance upon any information we provide and exclude liability for the statistical content to fullest extent permitted by law.