March 2023 **Industry snapshot**

Cybersecurity report

Inside: Market highlights · Deal volumes · Key players · About Clairfield

clairfield

2022 overview

clairfield

Joseph Sabet
Head of cybersecurity practice
jsabet@clairfield.com

Despite hopes of a return to some normality in 2022, the year provided a challenging climate in the cybersecurity space. Interest rate hikes and Russia's war on Ukraine, amongst others, set the tone for an extremely rocky cyber environment. Consolidation and roll-ups continued to be a popular play, with M&A proving to be a more attractive exit option given the volatile public markets.

Global cyber attacks increased by 38% in 2022 according to Checkpoint. This increase has been underpinned by the continued evolution of the ransomware ecosystem, with ransomware attacks growing 130% in 2022. Further, these attacks have become far more sophisticated, taking 49 days longer than the average cyber attack to identify.[1] The year also saw hackers widening their aim to target business collaboration tools, a rich source of sensitive data given the remote work climate. Following their post-Covid digitization, academic institutions proved a heavy feeding ground for cyber attacks, with the education/research sector seeing a 43% increase in 2022. Similarly, the healthcare sector's lack of cybersecurity resources has resulted in an 86% increase in attacks compared to that of 2021.[2] All of the above has set the scene for a much tougher Cyber Insurance climate too, with Forbes reporting that insurers have increased premiums by 79% and further decreased coverage.

As tensions rise in various regions worldwide, the potential for politically motivated cyber attacks increases. The recent initiation of conflict in Ukraine by a cyber attack on a commercial satellite internet network, further emphasized by Russia's ongoing cyber offensive against Ukrainian infrastructure, serves as a cautionary example. This threat makes it imperative for organizations to stay informed about the latest cybersecurity trends and invest in robust measures to defend against potential attacks.

Ransomware as a Service continued to establish itself as a fully-fledged industry in 2022, with double-extortion schemes posing enterprise risk from all angles. Manufacturing was impacted greatly by the pandemic, and further by the war. As the sector takes steps towards recovery, it continues its path towards digital transformation. Indeed, 2022 proved just how important cybersecurity will need to be in the future of global smart manufacturing.

Cybersecurity valuations were down throughout 2022. In 2022, cybersecurity acquirers paid roughly 7X revenue multiples, compared to 2021's 11.3X. Such declines are further evident in the Cybersecurity Hack ETF's 29% decline, underperforming the broader market by 10%.[3]

Trends in cybersecurity (1/2)

clairfield

IOT Devices have introduced new vulnerabilities to the market. It is expected that in 2023, there will be 43 billion IOT devices connected in the world. Ranging anywhere from smart wearables, home appliances, cars, alarm systems, and industrial machinery. A key reason for IOT devices getting hacked is because, as they are often not used to store sensitive data directly, manufacturers haven't always been focused on keeping them secure with frequent security patches and updates. Therefore, attackers go through the IOT devices and use them as gateways to access other networked devices that might help them lead through API's.

Multi-factor authentication (MFA) is a crucial component of a strong identity and access management (IAM) policy that requires multiple verification factors to access a resource. Its increased adoption in 2022 highlights the importance of protecting against identity theft, a growing threat that cyber criminals use to gain access to an organization's sensitive data. MFA enhances security by requiring additional verification factors, such as a thumbprint or physical hardware key, reducing the likelihood of successful cyber attacks. Implementing MFA helps build confidence within the organization that they will stay safe from cyber criminals and secure their sensitive data. It is considered one of the best ways to protect against identity theft and secure an organization's sensitive data in the face of the growing trend of cloud migration.

API Security - An API, or Application Programming Interface, is a set of protocols and tools for building software and applications. The adoption of APIs has increased dramatically in recent years and they are becoming the backbone of the internet. An API is a valuable target for cybercriminals because they're a backdoor for hackers to access vast amounts of business-critical data. The vulnerabilities hackers can use to exploit APIs are also on the rise, with insecure development practices being one of the key drivers. It is, therefore, imperative to implement proper authentication and access controls, regularly update the API and its dependencies, and monitor the API usage for any suspicious activities.

Phishing Schemes - This type of attack involves hackers using fraudulent emails or other communications to trick victims into revealing sensitive information, such as login credentials or financial information. Clicking on a fraudulent link can give the hacker access to the user's system, thereby creating an entry point for the exfiltration of sensitive data or the deployment of ransomware. Nearly 22% of all data breaches are accounted for by phishing[4]. In order to prevent this occurrence, it is crucial to educate employees on how to recognize phishing attempts, implement strict email security policies and technologies, and encourage employees to report suspected phishing emails.

Trends in cybersecurity (2/2)

clairfield

Ransomware is a type of malicious software that encrypts the victim's data and demands a ransom payment in exchange for the decryption key. Checkpoint revealed that the average ransomware attack cost companies a total of $4.54 million. The emergence of Ransomware as a Service (RaaS) has made it even easier for cybercriminals to deploy ransomware attacks on a larger scale, creating a much bigger threat for individuals and organizations. With RaaS hackers can purchase or rent pre-built ransomware tools, allowing them to launch attacks without the need for advanced technical skills. To protect against ransomware, organizations should implement multiple layers of security, such as anti-malware software, firewalls, and employee training on how to identify and avoid phishing scams. In addition, organizations must also have a disaster recovery plan in place, including regular backups and testing to ensure that critical data can be restored in the event of an attack.

CSPM – also known as cloud security posture management, automates cloud security management. Companies today, mistakenly assume that their cloud providers are responsible for their security when in fact they're not. Public cloud infrastructure is programmable through APIs, and hackers can easily gain access to the enterprise cloud. CSPM solutions continuously and autonomously monitor the cloud infrastructure for any misconfigurations that indicate such an attack and therefore are crucial in protecting cloud environments from bad actors.

AI–powered cybersecurity – As a result of the talent shortage in the cyber industry AI is being used in various ways to improve cybersecurity, such as detecting attacks more accurately, prioritizing responses based on real-world risk, and predicting future attacks. However, bad actors are also taking advantage of AI to identify weaknesses in software and security programs, create large numbers of phishing emails and malware that constantly changes to avoid detection. AI-powered malware can evade static defenses and sit inside systems collecting data with low risk of detection. While good AI defenses are difficult to build, the use of AI in cyberattacks is growing, and it is likely that AI-powered attacks will become more sophisticated in the future.

Sources:
1.https://venturebeat.com/security/microsoft-cybersecurity-predictions/2
2. https://www.digit.fyi/38-increase-in-2022-global-cyber-attacks/
3.https://finance.yahoo.com/quote/HACK/
4. https://www.verizon.com/business/resources/reports/dbir/2020/summary-of-findings/

Cybersecurity M&A transactions

clairfield

Notable M&A transactions in 2022

Acquiror	Target	EV (US$ billion)
THOMABRAVO	SailPoint	6.9
Kaseya	datto	6.2
opentext™	MICRO FOCUS	6
Google	MANDIANT	5.4
VISTA EQUITY PARTNERS	KnowBe4 Human error. Conquered.	4.6
THE CARLYLE GROUP	ManTech Securing the Future	4.2
THOMABRAVO	PingIdentity	2.8
THOMABRAVO	ForgeRock	2.3

Most active investors in 2022

NEA New Enterprise Associates · Accel · SEQUOIA · intel capital · andreessen horowitz · INSIGHT PARTNERS · Bessemer Venture Partners · lightspeed · TIGERGLOBAL

PE firms active in buyouts

THOMABRAVO · THE CARLYLE GROUP · VISTA EQUITY PARTNERS

Cybersecurity companies taken private in 2022

ForgeRock · KnowBe4 Human error. Conquered.

Case study: Clairfield's UK partner advised on the sale of OGL Computer Support and CyberGuard Technologies to Wavenet

clairfield

IT services

OGL

was sold to

wavenet

Clairfield's UK partner advised on the sale of OGL Computer Support and CyberGuard Technologies, together a leading provider of IT Services and Cyber Security, to Macquarie Capital backed Wavenet.

"It has been a pleasure working with the Clairfield team. They showed great knowledge of the IT sector, identified a strategic buyer that was the right fit for our customers and employees, and managed the sale process professionally. I would have no hesitation in recommending them to anyone considering a sale of their business."
— Ashok Patel, group CFO

"We are delighted to have advised on the sale of OGL Computer Support and CyberGuard to Wavenet, a strategic acquiror providing an opportunity for the combined business to enhance its offering and grow at a faster pace."
— Shah Zaki, Clairfield partner

OGL Computer Support and CyberGuard are an eminent Midlands based IT Solutions and Cyber Security Services provider, employing over 200 staff with high profile clients in the private and public sectors. OGL Computer Support has been delivering first-class IT solutions to 1,000+ UK businesses for over 45 years and is accredited by the world's leading IT and Cyber Security vendors including, Microsoft, HP, WatchGuard and VMware. CyberGuard Technologies launched in 2017 and provides a suite of CREST- accredited Cyber Security Solutions.

Wavenet is a leading provider of Unified Communications including Telephony, Internet, Cloud, Security and Mobiles, supplying solutions to over 8,000 SME, enterprise and public sector customers.

Having made this strategic acquisition, Wavenet is now one of the largest providers of Unified Communication, Cloud Solutions and Cyber Security Services in the UK.

Clairfield role

Clairifield worked closely with the shareholders of OGL Computer Support and CyberGuard on the sale process.

Specifically, Clairfield led the following critical processes:

- Spent time with the shareholders to understand the unique selling points of the business and presented these to the buyer.
- Utilised our detailed knowledge of the business and the sector to identify Wavenet as a strong strategic buyer that was the right fit for OGL's customers and employees.
- Analysed the financials of the business and presented a detailed run rate analysis in order to maximise the value for the shareholders.
- Managed the preparation and flow of information throughout the diligence process to ensure commercially sensitive information was safeguarded.
- Ensured effective liaison and communication between both parties and all advisors throughout the deal process to deliver a successful outcome.
- Negotiated key commercial aspects of the legal documents to ensure the successful completion of the deal.
- Overall project management through to a successful conclusion.

Clairfield's deep cybersecurity experience

clairfield

Fintech

GBG

acquired

IDOLOGY

Fintech

profihost

was sold to

dogado

Internet services

CLOUDALLY
Secured Cloud Backup

was sold to

zix

IT services

GRAYSHIFT

received strategic growth investment from

THOMABRAVO

IT services

accenture

acquired

BCT Solutions

IT services

IMPACT PARTENAIRES

sold

SECURIVIEW
NEXT GENERATION SOC
A LINKBYNET COMPANY

to

LINKBYNET

IT services

Aurora

owner of rcs
BEHIND A SAFER WORLD

was sold to

CY4GATE
ELETTRONICA GROUP

IT services

Management and

QUADRUM CAPITAL

acquired

DataExpert

IT services

OGL

was sold to

wavenet

Software & apps

alcea

was sold to

ASSA ABLOY

Software & apps

BOSS INDUSTRIES

sold

elektron

to

CHAPSVISION
DATA MAKE SENSE

Software & apps

GRAYSHIFT

completed a minority growth recapitalization with an investor group led by

PEAKEQUITY PARTNERS

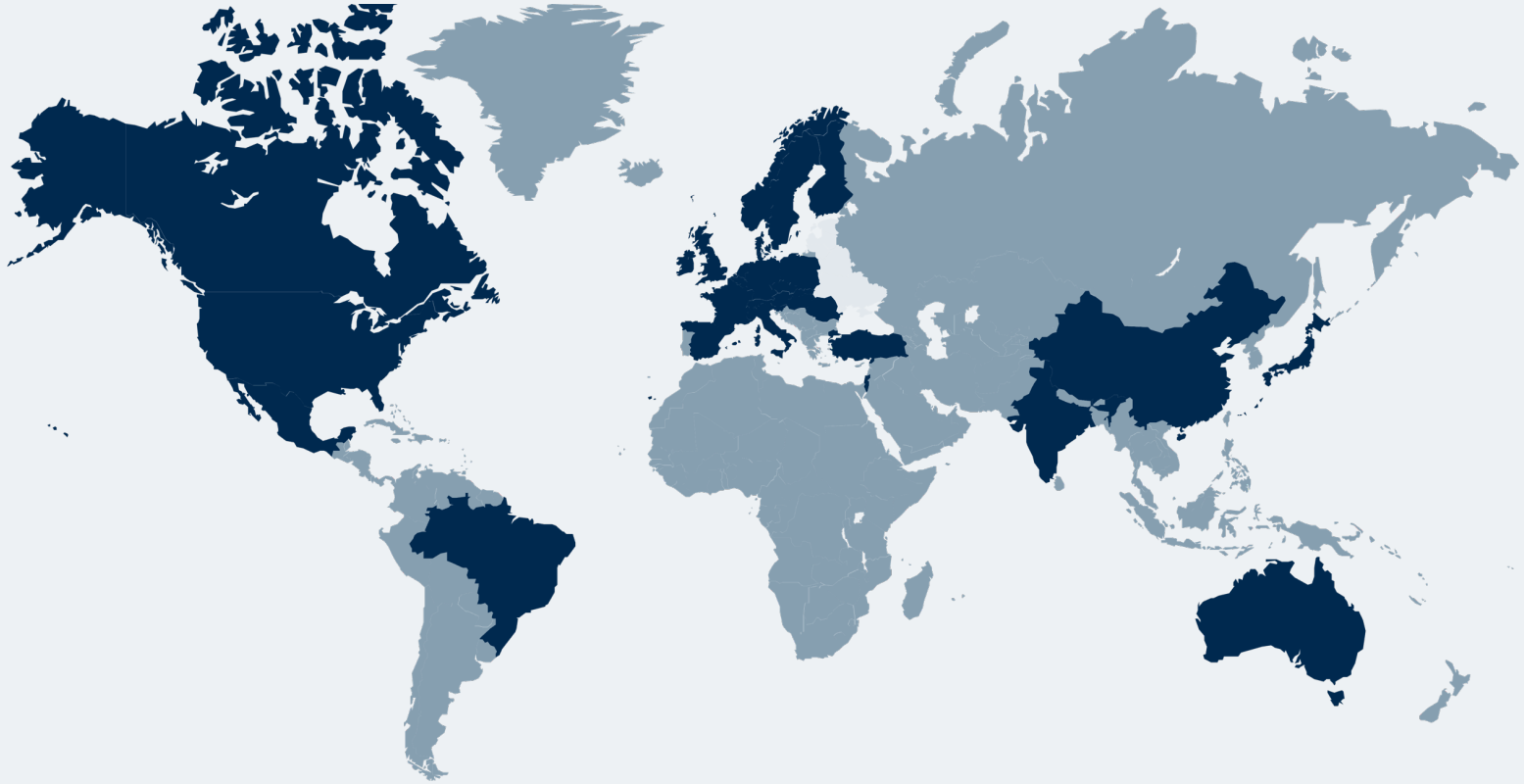
The tech, software & digital team at Clairfield

clairfield

+70
Team members

+330
Sector transactions closed since 2006

+EUR 8.5 bn
Cumulative value of sector transactions closed since 2006



CONTACT

Joseph Sabet
Head of cybersecurity practice
jsabet@clairfield.com
T: +972 3 607-4100

Bertrand Hermez
Head of tech, software & digital sector group bhermez@clairfield.com T: +33 1 40 20 12 34

Clairfield International (www.clairfield.com) provides advisory services on middle-market transactions for large companies, private investors and private equity, public sector clients, and family businesses. Headquartered in Europe with locations in every major region worldwide, Clairfield offers clients access to local corporate businesses, investors, and key decision makers, combined with a deep understanding of local regulations and cultures. Clairfield ranks as one of the top independent M&A advisors in league tables worldwide.

For more information on Clairfield, contact:
press@clairfield.com

www.clairfield.com