nccgroup

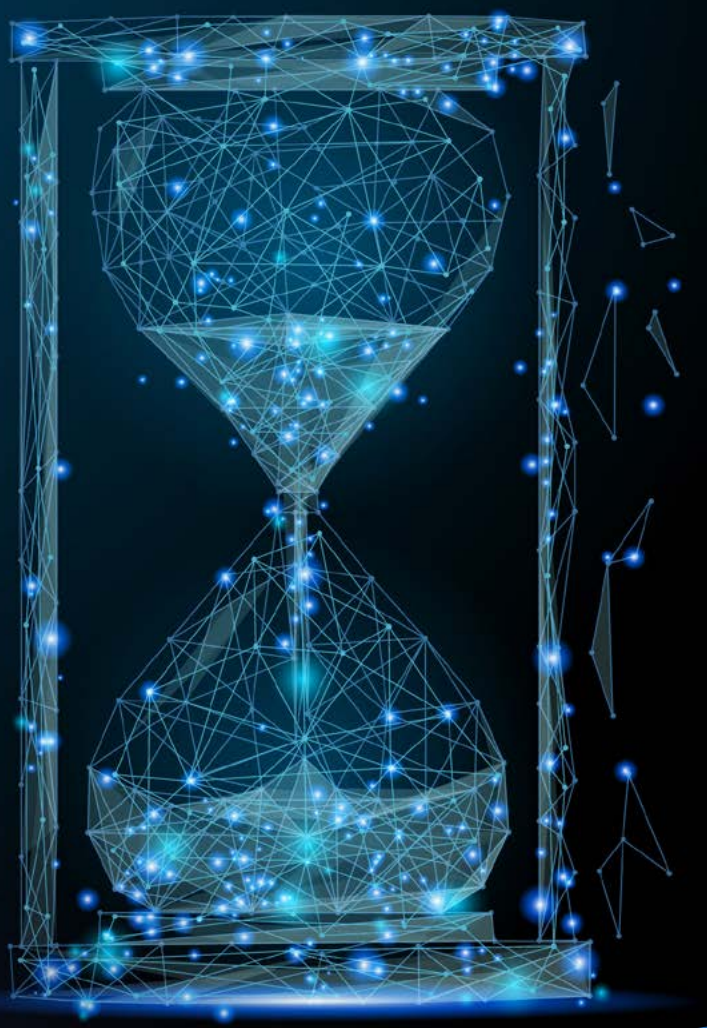
FOX IT
part of nccgroup

Insights

Pragmatic cyber security advice for senior executives

The shifting sands of cyber threats

Market Research Report



- The volume of cyber attacks are increasing
- Crimewatch: The most prolific cyber-criminal groups
- Spending plans and bolstering response

How companies are fighting back against a rising tide of cyber incidents

Global. Transformative. Resilient.

The shifting sands of cyber threats

How companies are fighting back against a rising tide of cyber incidents

Cyber security incidents around the world are evolving. Hackers are shifting shape, regrouping, disbanding or springing up anew. The types of attack are becoming more sophisticated or targeting new victims, increasing sharply in the first half of this year, led by a new strain of ransomware, followed closely by a continued boom in phishing, malware and denial of service attacks.

And with the geopolitical landscape in flux as the Russia-Ukraine conflict continued, many organisations were caught in the crosshairs of nation state-sponsored attacks.

Yet, as threat actors and attack types adapt, so too are organisations' ability to respond.

In this issue of Insights, we examine how cyber-security threats are changing and which industries are most at risk for potential attack. You'll hear from our experts, giving tips for how companies can identify and mitigate shifting cyber security threats.

We focus on two separate pieces of research and analysis, which provide an intriguing snapshot into the cyber security threats faced by companies and how they are prioritising their defences.

Research one was a survey commissioned by NCC Group, between December last year and January this year. It questioned nearly 1,400 cyber security decision makers in countries across the globe, including the United Kingdom, United States, China, Germany, and Singapore.

Research two was analysis by NCC Group's Threat Intelligence team, the Threat Monitor report, into critical cyber security incidents worldwide between April and June.

61%

of cyber security professionals around the world said that the number of cyber security threats their organisation had encountered had increased in the past year

Cyber security incidents around the world are evolving. Hackers are shifting shape, regrouping, disbanding or springing up anew.

The volume of cyber attacks are increasing

Six in ten (61%) of cyber security professionals around the world said that the number of cyber security threats their organisation had encountered had increased in the past year.

In the second quarter of 2022 ransomware attacks worldwide increased by 12%, compared to the previous quarter, according to our Threat Monitor analysis in the second quarter of this year.

Taking a regional view, in the first quarter of this year there was a noticeable rise in European-based activity, with the continent the most targeted for attack. Based on this quarter's data, it seems this was a temporary anomaly, likely as a result of the Russia-Ukraine conflict. After the initial surge in European-targeted attacks, North America returned to the 'top' target spot with 269 attacks recorded between April and June (42%), as compared to 244 in Europe (36%) and 89 in Asia (14%).

12%

increase of ransomware attacks worldwide in the second quarter of 2022 compared to the previous quarter

Types of attack

No surprise here. Ransomware continues to be the most common type of cyber attack, according to our analysis of critical cyber security incidents worldwide between April and June, responsible for 63% of all cyber security incidents.

Technology is making ransomware cheaper and more accessible.Almost half (47%) of these ransomware cases were conducted employing off-the-shelf technology tools.

63%

of all cyber security incidents worldwide between April and June continues to be ransomware

45% increase in **insider threats**

48% increase in **denial of service attacks**

49% increase in **ransomware attacks**

51% increase in **supply chain attacks**

60% increase in **phishing & malware attacks**

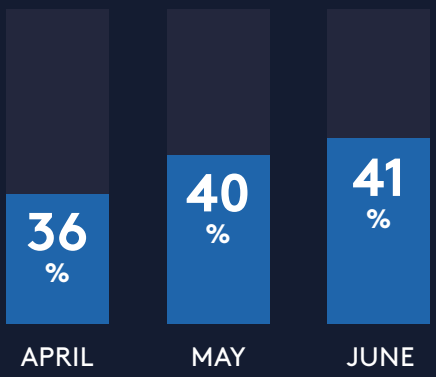
Initial access was most often achieved using vulnerable external facing servers (**37%**) followed by malicious emails with links or attachments (**32%**)

> To find out more about optimising these defences, head to page 14.

Crimewatch: The most prolific cyber-criminal groups

Corporate cyber security in the second quarter of 2022 has been dominated by three ransomware gangs: **LockBit2.0, Conti and BlackCat**.

RANSOMWARE INCIDENTS



LockBit

LockBit2.0 – a type of ransomware that targets Windows PCs and now Linux servers – remained the most prominent threat actor in the second quarter.

Over the three-month period, the number of LockBit2.0's attacks fluctuated. In April, the ransomware strain accounted for 36% of all ransomware incidents, 40% of overall ransomware or cyber security incidents in May and 41% of all incidents in June.

The decline was likely due to cyber criminals preparing a new strain – LockBit3.0.

Industrials was the most targeted sector for ransomware attacks, followed by consumer cyclicals, and technology.

Want to find out how LockBit are shifting shape?
Read our Spotlight on page 20.

16%

In April, Conti was responsible for 45 out of 289 incidents

Conti

The second most prolific ransomware group put Costa Rica under siege for several months earlier this year and, according to Wired magazine, "rewrote the rules of cybercrime".

Conti, which recently shut down its operations, accounted for around 10% of total ransomware incidents between April and June.

In April, Conti was responsible for 45 out of 289 incidents (16%). In May it accounted for 7% of all ransomware incidents, and just 1% in June. The group's activity has seen rapid decline – suggesting its members have re-grouped alongside Conti affiliates and new ransomware strains.

8%

BlackCat accounted for 8% of total ransomware incidents in the second quarter

BlackCat

The third main ransomware gang made a strong start to the year. As of March, it had breached the security of at least 60 organisations around the world, according to the Federal Bureau of Investigation (FBI).

BlackCat accounted for 8% of total ransomware incidents in the second quarter.

As with LockBit2.0 and Conti, BlackCat targeted three sectors – industrials, followed by consumer cyclicals and technology.

Spending plans and bolstering response

So, how are companies responding to changing cyber-security threats? Our research paints a mixed picture of company cyber security.

Companies said that they were able to respond faster to cyber security incidents (84% said they could respond within one day), with seven in ten reporting their ability to respond quickly and effectively had improved in the past year. However, only 34% of those questioned rated their organisation's cyber security as "very resilient".

So where do priorities lie, when it comes to cyber resilience? When cyber security professionals were asked for their spending plans for the next six months to one year, threat detection and response was top (32%), followed by cyber security reviews and assessments (25%), and jointly security awareness and training, and security testing, infrastructure and application (24%).

In the same research, we asked companies if they planned to increase spending on cyber security in the next year, and if so, what they planned to spend the biggest proportion of the increase on.

Where do priorities lie, when it comes to cyber resilience?

32 %	Threat detection and response
25 %	Cyber security reviews and assessments
24 %	Security awareness, training, security testing, infrastructure and application

82% said they planned to increase spending on cyber security. Of those that did plan to increase spending, the biggest share of any increase was expected to go on managed security services, followed by cloud integrated security products, and hardware-based third-party security products.

RESEARCH SUMMARY

The number of cyber attacks against businesses are increasing, according to an NCC Group survey of approximately 1,400 cyber security decision makers at large companies in 11 countries, including the UK, United States, China, Germany and Singapore. The survey was conducted in December 2021 and January 2022.

Six in ten (61%) of cyber-security professionals around the world said that the number of cyber-security threats they had encountered had increased in the past year.

Ransomware continues to be the most common type of cyber attack worldwide, according to NCC analysis of critical cyber security incidents worldwide between April and June - responsible for **63%** of all cyber security incidents.

In the second quarter of this year, the most common cyber criminal group was the ransomware group LockBit 2.0, followed by two other groups – Conti and BlackCat. Ransomware groups form and disband quickly, sometimes within months.

About Insights

Insights is a program designed for sharing pragmatic cyber security insights with senior executives. You can expect a magazine and interactive online event about a trending topic each quarter. Register here for the free virtual Insights event: Growing Threats.

About NCC group

It's a new era of risk. Defy it with NCC Group's end-to-end cyber security and resilience solutions, and confidently embrace technology to support sustainable growth and success.

From governments to tech giants, financial institutions to expanding businesses, for over 30 years we have proudly provided them with strong security solutions...and with a global team of over 2,400 experts, we're ready to do the same for you.

With NCC Group, take your business to the next level. Unleash innovation without the obstacle of cyber threats.

More than a solution. **A partner.**

You're not alone on your security journey. NCC Group is your partner. Be it rolling up our sleeves with your in-house team or developing strategy with your board, we help you have control over your appropriate level of security. Yes, we deliver industry leading security solutions, but we'll also reduce stress, save your business time, and help you prepare for, or even face, a crisis together.

www.nccgroup.com

UNI106269