Carbon Black.

UK THREAT REPORT

Hacking, Escalating Attacks and the Role of Threat Hunting

This research was conducted to understand the challenges and issues facing UK businesses right now in their fight against cybercrime including hacking, malicious attacks, and breaches, and to scope how organisations are using threat hunting to strengthen their defences.

SEPTEMBER 2018

Survey Methodology

Carbon Black commissioned a survey, undertaken by an independent research organisation, Opinion Matters, in August 2018. More than 250 UK CIOs, CTOs and CISOs were surveyed from companies in a range of vertical industries including: financial, healthcare, government, retail, manufacturing, food and beverage, oil and gas, professional services, and media and entertainment.

Foreword

THE MODERN ATTACK LANDSCAPE IN THE UK

Tom Kellermann
Chief Cybersecurity Officer, Carbon Black

Rick McElroy
Security Strategist, Carbon Black

The research presented in the report below shows that a staggering 92% of UK businesses have been breached in the past year and nearly half of UK companies reported falling victim to multiple breaches (3 to 5 times in the last year.) Pause for a moment to read those numbers again. Nearly 100% of UK businesses report being breached during the past 12 months with half of them reporting several breaches, which can potentially cripple an organisation.

Following a global trend, cyberattacks in the UK are becoming more frequent and more sophisticated, as nation state actors and crime syndicates continue to leverage fileless attacks, lateral movement, island hopping, and counter incident response in an effort to remain undetected.

This issue is compounded by resources and budgeting. Not only is there a major talent deficit in cybersecurity, there is also a major spending delta. It's estimated that the underground cybercrime community spends upward of $1 trillion annually on developing attacks. By comparison, worldwide

92% of UK businesses have been breached in the past year

businesses are spending about $96 billion to protect themselves. Defenders are being outspent by a ratio of 10 to 1 – another staggering and sober statistic.

Carbon Black also recently conducted a threat survey of global incident response (IR) professionals, the Quarterly Incident Response Threat Report (QIRTR), which highlights how attacks are evolving. In this report **64% of IR professionals noted** they were seeing secondary command and control occurring as attackers launched hidden secondary payloads after the initial attack had been shut down. Furthermore, 46% of IR pros had found evidence of counter incident response from adversaries. Attackers are increasingly reacting and adapting to defenders' response efforts.

In light of these concerning developments, what can UK businesses do to redress a situation where, at present, adversaries hold a distinct advantage? **Cybercrime groups are better funded, greater in number, and acting with increased sophistication.** Defenders need to act now before the risks become untenable.

There is a silver lining in our research. Two thirds of UK organisations said they have pro-actively conducted threat hunting in the past year to strengthen their defences. Within companies that actively threat hunt, more than 90% said threat hunting had toughened their defences. This is certainly a positive sign.

Proactive threat hunting is an essential activity in today's threat armoury. A multidisciplinary team should be anticipating the potential weaknesses and viable attack paths not just within the organisation, but across the information supply chain, to get a step ahead.

In today's digital environment success is less about waiting for the inevitable attack and more about **establishing enterprise visibility**, augmented by threat hunting and intelligent incident response, plus ensuring that we are deploying protection mechaniams that can detect and stop advanced attacks.

With this research, we wanted to find out if UK organisations are seeing an increase in attacks and if those attacks are becoming more sophisticated. The answer to both those questions was **overwhelmingly, "yes."** We were also keen to find out what respondents thought were the most effective and destructive types of attacks, including island hopping and new vulnerabilities caused by an insecure supply chain. The full findings from those queries, and more, **appear in the report below**.

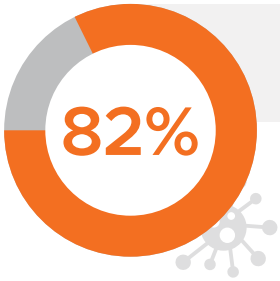
TOP RESEARCH FINDINGS

FREQUENCY OF ATTACKS

92% of UK businesses have been breached in the last 12 months, and almost half (44%) of these said their company had been breached multiple times (between 3 to 5 times).

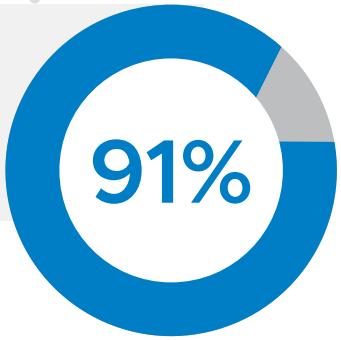
ESCALATING ATTACKS

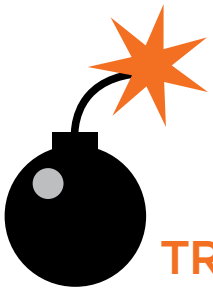
82% of UK respondents have seen an increase in cyberattacks on their company in the past 12 months. Over a quarter have seen up to a 25% increase in cyberattacks and 1 in 4 (26%) have seen somewhere between a 26% to 50% increase, with 27% having seen an increase anywhere from **51% to 200%.**



82% HAVE SEEN AN INCREASE IN
CYBERATTACKS

91% OF BUSINESSES BELIEVE CYBERATTACKS HAVE BECOME MORE
SOPHISTICATED





$1
TRILLION

CYBERCRIMINALS

Are outspending defenders by a 10-to-1 ratio

Are spending an estimated **$1 trillion** on developing cyber weaponry. By comparison, defenders are spending about $96 billion. In our survey, only 1 in 20 UK businesses were aware of this major delta.

LIMITED UK BUDGET SPEND

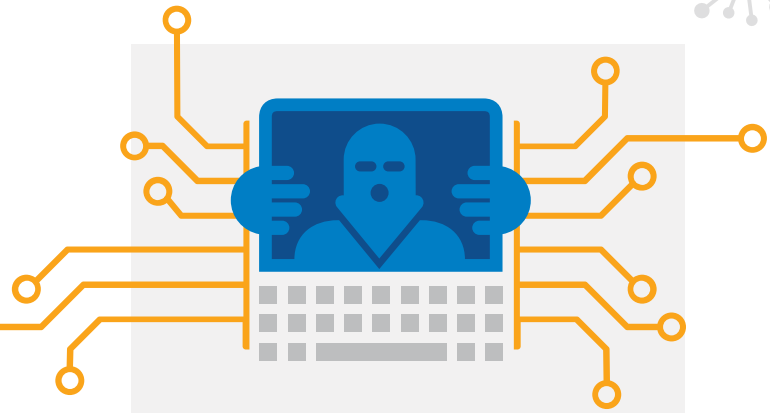
Almost two thirds **(63%)** of UK businesses said they were only planning on **increasing their budget spend** on cyber defence by between 11% and 30%. Surprisingly, 10% of UK businesses said they are not increasing spend at all.

WHICH ATTACKS CREATE MORE HAVOC?

The report highlights that 35% of data breaches were caused by either **phishing attacks or ransomware.** Nearly one quarter (23%) were the result of weak security processes or outdated security software.

Delving deeper to understand which types of attacks have been most prolific, commodity malware and ransomware topped the list with a combined 45%. Cryptojacking was the fourth most cited type of cyberattack.

Interestingly, **1 in 12 of the organisations surveyed** said that a breach in their supply chain was the most common attack they had suffered in the past year. When asked what they thought was the most effective and destructive type of cybercrime, over 1 in 3 businesses think DDOS and island hopping **(43%) create substantial havoc.**



35% of data breaches are caused by either phishing attacks or ransomware

THE ROLE OF THREAT HUNTING

When asked whether they had used threat hunting techniques to strengthen their defences, 1 in 5 organisations (22%) say they have threat hunted for more than a year, rising to 2 in 5 (43%) saying that they have started in the past year. Interestingly, within companies which actively threat hunt, over 90% said that it had toughened their defences.

FULL SURVEY RESULTS

HAVE YOU SEEN AN INCREASE IN CYBERATTACKS ON YOUR COMPANY IN THE LAST 12 MONTHS? IF SO, BY HOW MUCH?

82% of UK businesses have seen an increase in the number of attempted cyberattacks targeting their companies in the past 12 months

Over a quarter (26%) of businesses have seen **up to 25% increase in cyberattacks** on their company in the last 12 months.

Over 1 in 4 (26%) of businesses have seen **between 26 – 50% increase in cyberattacks** on their company in the last 12 months.

27% had seen an increase anywhere **from 51% to 200%.**

Over two thirds **(67%)** of businesses from the **utilities sector** (including oil, gas and telecoms) have seen up to a 25% increase in cyberattacks on their company in the last 12 months, as have over a third **(35%)** of **professional services** firms including law and accountancy, government and local authority (35%) and over a quarter **(27%)** in **financial services.**

INCREASED
ATTACKS

"It's critical to educate UK businesses on the threats they face and how these threats can be mitigated."

91% of UK businesses that had experienced a cyberattack on their company in the last 12 months said that the **attacks had become sophisticated,** leveraging techniques such as lateral movement, counter incident response and island hopping.

Three quarters of businesses **(75%) in the travel and transport sector** who had suffered a cyberattack on their business in the last 12 months said that they had become significantly more sophisticated.

60% of businesses employing between 10,001 – 20,000 employees who had had a cyberattack in the last 12 months said that cyberattacks had become significantly more sophisticated in that period.

HAVE CYBERATTACKS ON YOUR COMPANY BECOME MORE OR LESS SOPHISTICATED IN THE LAST 12 MONTHS?

SIGNIFICANTLY
SOPHISTICATED

Commodity malware, ransomware attacks and Google Drive (cloud data breach) **topped the list with a collective 45%**.

Malware and ransomware rose to almost two thirds **(60%)** within respondents from the **healthcare sector** as being the most prolific type of cyberattack.

Cryptojacking was the fourth most cited prolific attack type **(9%)** which doubled to **18%** in companies with 10-20 UK based IT specialists.

13% of businesses employing over 100,000 employees said that a **breach in their supply chain** was the most prolific type of attack they experienced.

WHAT HAS BEEN THE MOST PROLIFIC TYPE OF CYBERATTACK YOUR COMPANY HAS EXPERIENCED IN THE LAST 12 MONTHS?

13%
BREACHES IN
SUPPLY CHAIN

Note: Some subgroups contain a base size of less than 50 and should be treated as indicative.

HOW OFTEN HAS YOUR COMPANY BEEN BREACHED BY A CYBERATTACK IN THE LAST 12 MONTHS?

92% of businesses reported experiencing a **data breach** during the past 12 months.

Almost half (44%) of UK businesses said their company had been breached **3 - 5 times in the last 12 months.**

10% of healthcare organisations said their company had been breached over **10 times in the last 12 months.**

1 in 4 businesses with more than 100,000 employees said they'd **been breached 10 times.**

39% of companies with less than **10 UK based IT specialists** said they'd been breached once or twice.

WHAT WAS THE PRIME CAUSE OF THESE BREACHES?

35% of these data breaches were caused by either phishing attacks or ransomware. **Phishing attacks** topped the list at **18%**, very closely followed by **ransomware** at **17%.**

23% of respondents said the prime cause of attacks was either that their **processes were not** as strong as they thought they were, or that their **security was out of date.**

18% of businesses from the media and entertainment sector said a breach in the **supply chain** was the prime cause of the breach.

In companies that employ over 100,000 people, **25%** said that their **processes were not as strong** as they thought they were.

In companies with **less than 10** UK based IT specialists, **33%** said that phishing attacks were the prime cause, while in companies with **more than 100 UK-based** IT specialists the top reason was cited as **ransomware.**

"There is a silver lining in our research. Two thirds of UK organisations said they have pro-actively conducted threat hunting."

Interestingly, almost two thirds **(63%)** of UK businesses said they were only planning on **increasing their budget** spend on cyber defence by between **11% and 30%.**

10% said they are not **increasing spend** at all and **1%** even said they are going to **decrease expenditure.**

The sectors that are increasing spend the most are **travel and transport and media and entertainment** at **20% and 15%** respectively.

13% of companies with more than **100,000 employees** are **not planning to increase their budget spend** on cyber defence in the next year.

Companies with between **251 and 500 employees are devoting the most budget** to cyber defence with **28%** saying they would increase budget by between **41% and 50%.**

41% of companies employing **less than 10** UK based IT specialists said they are **not planning on increasing the amount they spend on cyber defence** in the next 12 months.

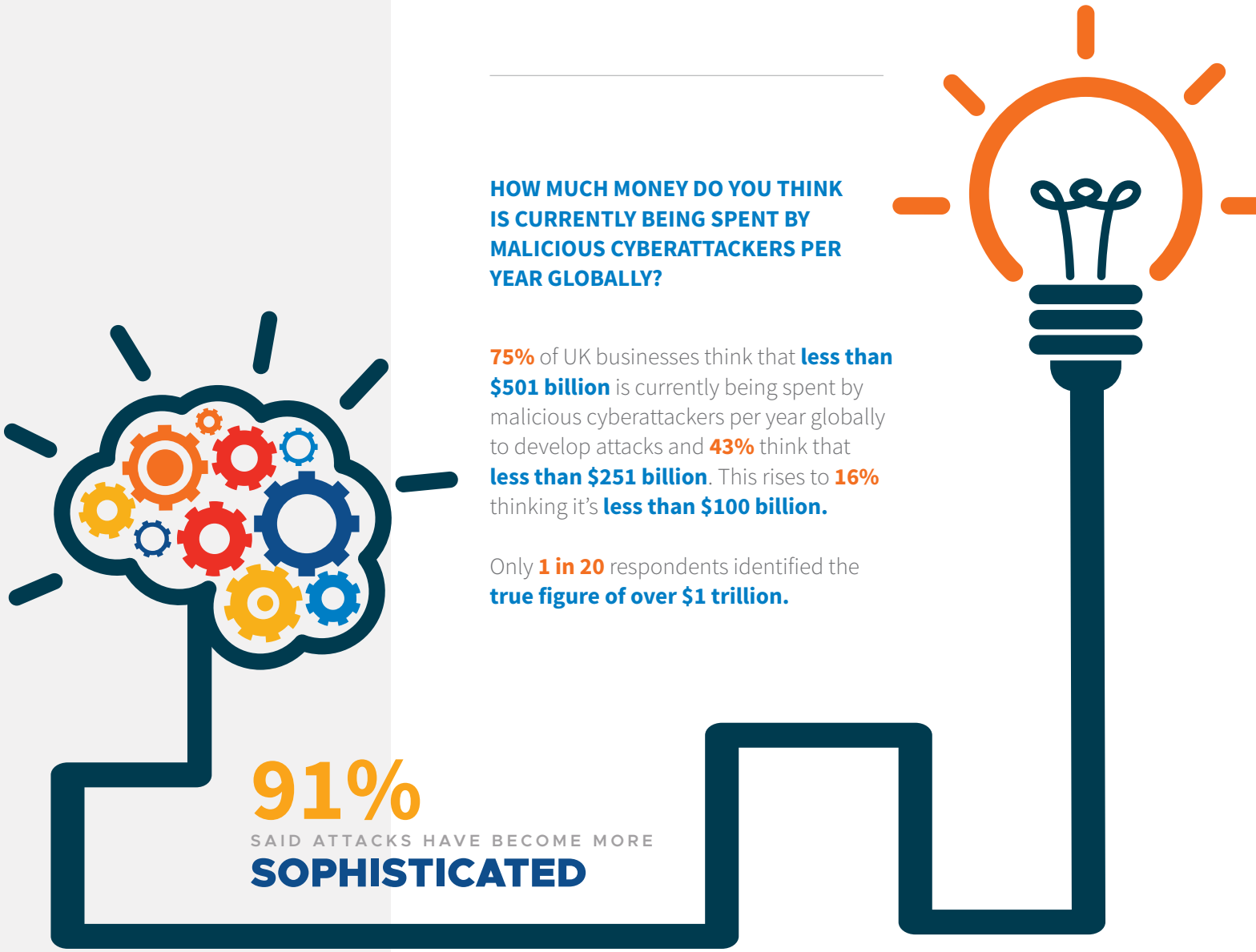
HOW MUCH ARE YOU PLANNING TO INCREASE YOUR BUDGET SPEND ON CYBER DEFENCE IN THE NEXT 12 MONTHS?

HAVE CYBERATTACKS ON YOUR COMPANY BECOME MORE OR LESS SOPHISTICATED IN THE LAST 12 MONTHS?

91% of UK businesses that had experienced a cyberattack on their company in the last 12 months said that the **attacks had become sophisticated,** leveraging techniques such as lateral movement, counter incident response and island hopping.

Three quarters of businesses **(75%) in the travel and transport sector** who had suffered a cyberattack on their business in the last 12 months said that they had become significantly more sophisticated.

60% of businesses employing between 10,001 – 20,000 employees who had had a cyberattack in the last 12 months said that cyberattacks had become significantly more sophisticated in that period.



HOW MUCH MONEY DO YOU THINK IS CURRENTLY BEING SPENT BY MALICIOUS CYBERATTACKERS PER YEAR GLOBALLY?

75% of UK businesses think that **less than $501 billion** is currently being spent by malicious cyberattackers per year globally to develop attacks and **43%** think that **less than $251 billion**. This rises to **16%** thinking it's **less than $100 billion.**

Only **1 in 20** respondents identified the **true figure of over $1 trillion.**

WHAT DO YOU THINK IS THE MOST EFFECTIVE AND DESTRUCTIVE METHOD OF CYBERCRIME?

Just over 1 in 5 UK businesses think **DDoS (22%)** and **island hopping (21%)** are the most effective and destructive methods of cybercrime.

42% of healthcare organisations think **DDoS** is the most effective and **destructive method of cybercrime.**

Island hopping has relatively low recognition – from **13%** within companies with less than 10 UK based IT specialists through to **27%** in companies employing 31-40 UK based IT specialists.

HAS YOUR COMPANY 'THREAT HUNTED' IN THE LAST 12 MONTHS?

22% of companies (or 1 in 5) say they have threat hunted for **more than a year,** rising to 2 in 5 **(43%)** saying they have started **in the past year.**

8% of companies say that **budget limitations** mean they can't employ independent threat hunters.

Over two thirds of people **(69%)** who work in the **media and entertainment industry** think the techniques they have in place are sufficient protection against a cyberattack.

Interestingly, a small **4%** of companies would **prefer to wait for attack, evaluate it and then respond,** yet less than half of companies are actively threat hunting.

38% of companies with more than 100,000 UK based employees **feel the techniques in place are sufficient protection.**

43%
HAVE THREAT HUNTED IN
THE PAST YEAR

IN THE LAST 12 MONTHS HAS YOUR THREAT HUNTING ACHIEVED YOUR GOAL OF STRENGTHENING YOUR COMPANY'S DEFENCES AGAINST CYBERATTACK AND FOUND MALICIOUS CYBERATTACK ACTIVITY YOU WOULD NOT HAVE ORDINARILY FOUND?

Within companies which **actively threat hunt,** over **90%** said that it **strengthened their company's defences.**

The sector that threat hunting has helped the most is the **travel and transport sector** with **100%** saying that **threat hunting has strengthened their defences.**

Threat hunters have had most efficacy in companies that have **over 50,000 UK based employees** with **80%** saying it strengthened their defences.

This is also the case within companies that employ **over 100 UK based IT specialists** – **60%** say it strengthened their defences.

ABOUT CARBON BLACK

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security. Carbon Black serves more than 4,300 customers globally, including 35 of the Fortune 100. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV). Leveraging its big data and analytics cloud platform – the CB Predictive Security Cloud – Carbon Black solutions enable customers to defend against the most advanced cyber threats, including malware, ransomware, and non-malware attacks. Deployed via the cloud, on premise or as a managed service, customers use Carbon Black solutions to lock down critical systems, hunt threats, and replace legacy antivirus.

Carbon Black.

Carbon Black
The White Building
1st Floor, Reading
Berkshire
RG1 3AR
T: 01189 082374

carbonblack.com