deep instinct

2021

Annual Study

Voice of **SecOps**

Introduction

The threat to businesses from cybercrime is increasing at a phenomenal rate around the globe. Ransomware has emerged as the central pillar of cybercriminal strategy. It has recently been predicted that a business will fall victim to a ransomware attack every 11 seconds, up from every 14 seconds in 2019, making ransomware the fastest growing type of cybercrime[1].

The U.S. Justice Department has placed ransomware investigations on the same plane as terrorism probes. Following the Colonial Pipeline attack, The White House has now issued a series of new cybersecurity requirements for gas pipelines.

And in the UK the government's National Cyber Security Centre handled more than three times as many ransomware incidents in 2020 as in 2019[2].

It's been estimated that the cost of ransomware incidents worldwide is expected to spiral out of control, soaring to more than $265 billion by 2031.[3]

But it's not just ransomware that is a key worry for the cybersecurity community. Viruses, SQL injections, DDoS attacks, and the like have not gone away – these threats still remain significant security risks for organizations. And to add to the complexity of guarding against cyber threats, the massive increase in remote working in the wake of COVID-19 has seen an exponential increase in the number of remote business endpoints that CISOs are being asked to secure.

Estimated cost of ransomware incidents by 2031

$265 BILLION[4]

In April / May 2021 The Hayhurst Consultancy was commissioned by Deep Instinct to conduct research among 600 cybersecurity professionals across North America and Key Western European countries. Deep Instinct spoke to C-Suite cybersecurity decision makers and their senior team members - including CISOs, CTOs, global cybersecurity leads, and infosec analysts across a range of key verticals - including technology, financial services, healthcare, telecoms, and manufacturing. The goal of the research study was:

- The key current threat concerns in the cybersecurity community
- The efficacy (or otherwise-) of existing solutions available to the community
- Where the cybersecurity industry needs to put focus in order to provide a future-proofed cybersecurity solution that goes beyond traditional AI/ML solutions

All respondents are employed by businesses with revenue of at least US$500M, employing more than 1,000 staff. Full details of the sampling are provided in the appendix.

Management Summary

The cybersecurity community knows it faces increasingly innovative cyber threats on a variety of fronts.

They recognize that cybercriminals are ruthless and well-funded – often better-funded than those seeking to defend against them - and are therefore able to harness the very latest technologies to conduct their criminal operations, sometimes with the support of their own host government.

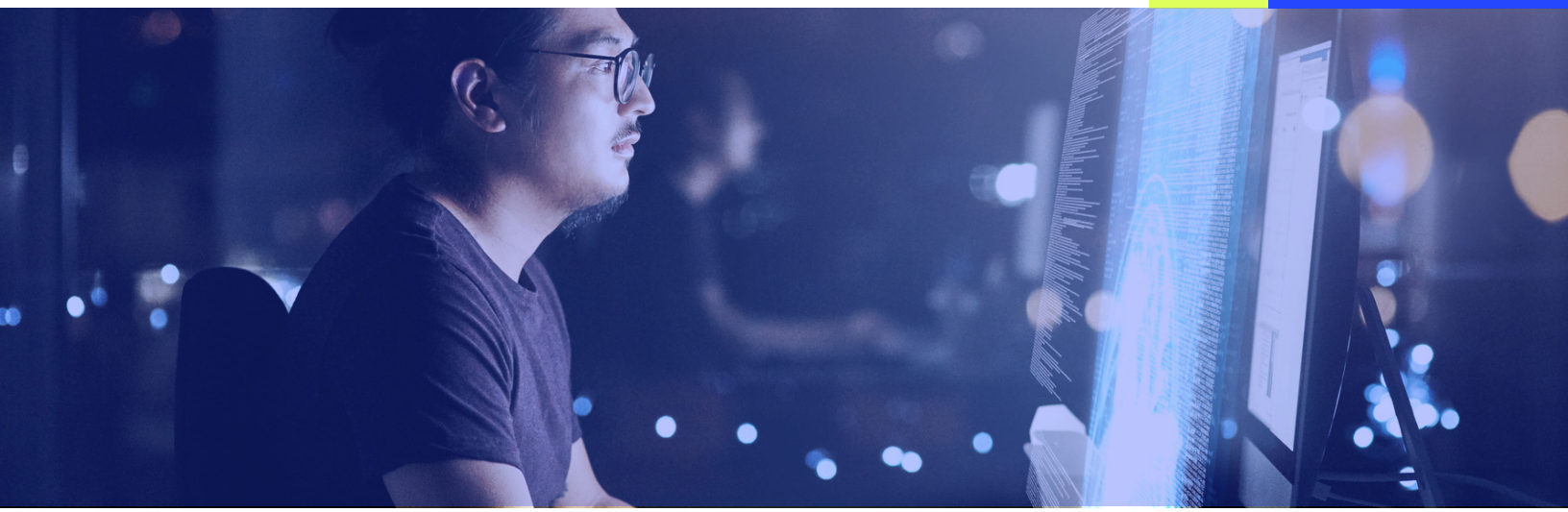
Our survey found that cybersecurity professionals admit they are struggling to cope with how fast-moving the criminal fraternity has become.

There is widespread dissatisfaction with some current cybersecurity solutions, which are seen to be:

- Ineffective against novel threats
- Inefficient to manage
- Time consuming
- Resource intensive
- Generating masses of data that is expensive and exhaustive to monitor

It is the responsibility of cybersecurity solution vendors to develop innovative, effective defenses that:

- Are primed to prevent zero day attacks
- Dramatically reduce - if not eliminate - false positives
- Provide certainty against ransomware
- Ensure minimal impact on a customer's IT landscape
- Provide easy integration with existing tools
- Require minimal updates and patching, if any
- Are highly automated
- Can be delivered ideally by a self-learning, intelligent AI that is highly effective in separating the threat signal from the false-positive noise
- Pay for themselves through by cost savings generated in the Security Operations Center (SOC) via false positive elimination or reduction



Identification & ranking of threat concerns

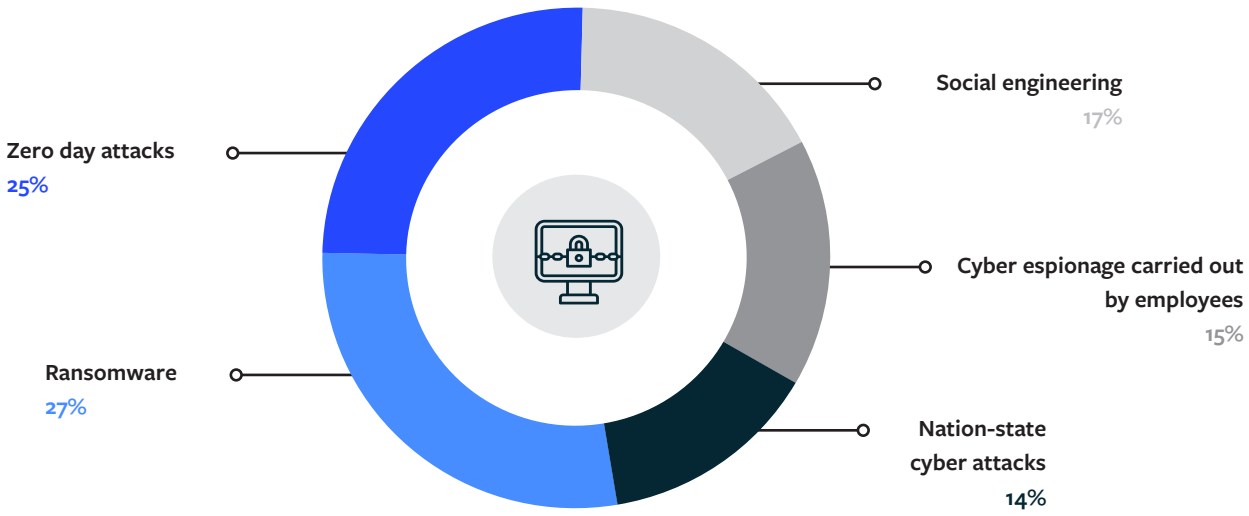
The research data strongly suggests CISOs are increasingly having to play 'whack-a-mole' with a range of key cyber threat concerns; this is impacting their ability to focus resource allocation, meaning already over-stretched cybersecurity teams are being spread even more thinly.

In the survey, respondents were invited to rank five key cybersecurity threats, starting with those most concerning to their business. While ransomware was the most likely to be ranked the primary concern, almost as many respondents ranked zero-day attacks as what they saw as their top threat.

Despite being the least cited #1 threat, nation-state attacks still ranked in the top 3 most concerning threats by almost half of respondents (45%).

Rank the following types of threats for your company from most concerning to least

Percent of respondents ranking each threat #1



The Solar Winds attack provides further evidence that cybersecurity teams are being pulled in multiple directions and are requiring more staff to prepare for future threats. More than 90% of respondents have seen some kind of response within their organization, and 55% have said that the attack has prompted more questions at the board level about cybersecurity readiness.

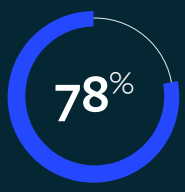
Yet despite the above efforts to staff-up to mitigate the increasing wave of threats, there is a growing expectation that the chances of a successful criminal attack on North American respondents' business is rising in likelihood, not falling. 42% of respondents state that it is much more likely that a successful ransomware attack on their company by criminals will take place, and 30% believe an attack is slightly more likely.

42% of respondents state that it is much more likely that a successful ransomware attack on their company by criminals will take place

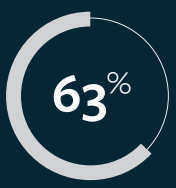
30% believe an attack is slightly more likely

Similar patterns are seen on the other side of the Atlantic

In Germany, only 15% of respondents believed that their level of concern... in terms of ransomware and other threats has decreased in 2021



In the UK, 78% of respondents agreed that "I'm concerned that sophisticated cyber adversaries will develop and deploy true artificial intelligence to cause a global incident in the next 12 months."



In France, 63% of respondents agreed that "humans can't keep up with the exponential pace of cybersecurity threats."

Frustration with existing solutions

It comes as something of a surprise to discover that these increased concerns over cybersecurity threats to business are not currently being matched by the efficacy of many of the traditional solutions available to cybersecurity professionals:

83% of the 600 cybersecurity professionals we spoke to agreed that **"Cybersecurity professionals deserve better from their Anti-Virus and Endpoint Detection and Response solutions."**

It's not that better solutions aren't always available. This widespread frustration that cybersecurity professionals are fighting a losing battle with outdated tools is also reflected by the fact that:

84% of the 600 cybersecurity professionals we spoke to agreed that **"I believe there are tools available in the cybersecurity market that could improve my company's defenses"**

The frustrations identified by cybersecurity professionals extend in particular to Endpoint Detection and Response (EDR) solutions.

While 72% of respondents claimed to have an EDR in place, as many as 67% of those respondents expressed some lack of confidence in their existing solution.

Interestingly, there was some evidence to suggest that C-Suite respondents had greater confidence in their EDR than their direct reports who actually have to run them day-to-day, pointing to potential complacency about some of the solutions under the C-Suite's remit.

So, what are the frustrations with legacy processes that cybersecurity professionals are having to endure?

Patching is one:

84% of respondents agreed that "Our security technologies require frequent, time-consuming security patches and updates to ensure a solution remains effective"

The fact that some solutions only have a limited range of threat vectors they can monitor is another:

76% of respondents agreed that "some security solutions have a limited range of threat vectors they can combat, risking exposure to out-of-scope ones, or requiring additional vendors to fill the gaps"

The unpredictability of zero day threats is a third:

66% of respondents agreed that they "have concerns that zero day attacks can't be prevented when they have never been seen before"

AS MANY AS **67%** **of those respondents expressed some lack of confidence in their existing solution**

False positives – the key drain on management time

On top of the EDR frustration, there is a clear challenge with regards to the abundance of false positives, and how much time, resource, and budget must be spent dealing with them.

Ultimately, these shortcomings lead to a clear impact not just on the efficacy of cybersecurity solutions currently in play, but also on the people charged with managing them:

62%

62% of respondents agreed that **"threats in my company could get missed due to the overwhelming volume of false positives,"** and

69%

69% of respondents agreed that **"low staff morale could result from alert fatigue due to the overwhelming volume of false positives"**

The lost time dealing with false positives impacts all levels of the SecOps organization:

On average, each cybersecurity professional we spoke to claimed to spend 9 hours, 40 minutes each week "dealing with alerts caused by false positives"

U.S. respondents spent significantly more time than their non-U.S. peers dealing with alerts caused by false positives - on average 10 hours, 54 minutes a week (more than 1 hour more each week)

This phenomenon wasn't limited to operational cybersecurity respondents either: while Information Security Analysts were amongst the most "put upon" personas (11 hours, 50 minutes per week, on average) the Global CISOs we spoke to weren't far behind (11 hours, 9 minutes per week on average).

The statistics suggest that if cybersecurity professionals had a tool to completely eliminate false positives they would save a quarter of their time – freeing it up to focus on the identification and prevention of upstream threats (rather than dealing with false alerts for threats that never actually existed in the first place).

Steps to address threats

A key strategy being adopted by businesses is the adoption of automated / AI-based cybersecurity solutions (65% of U.S. respondents indicated this was their business' response to the recent Microsoft Exchange zero-day attack).

It's scarcely surprising that some form of automation is perceived as a part of the solution when 83% of respondents agreed that "automation allows us to free up teams to focus on higher-value and / or more strategic tasks."

And 71% of respondents agreed in some way that "automation of cybersecurity is the only way our company can address cyber threats."

This is clearly because unautomated systems are inherently resource-inefficient.

In Germany, respondents were most likely to rate "Resource efficiency" (i.e., the extent to which the solution improves the efficiency of the people operating it) as the foremost criteria influencing an IT purchase within their company (31% of respondents).

However, automation alone is unlikely to ease these challenges other than in the very short term. It's clear that there has to be an intelligence behind the automation which will deliver the best efficiencies.

But what *kind* of intelligence is optimal?

Regional studies suggested that not all AI solutions are created equal. For example, only 1 in 4 French cybersecurity professionals believed that their AI solution was completely trustworthy.

Regional studies also provided to some intriguing pointers to how valuable a self-learning cybersecurity solution might be. Only 1% of German respondents thought that a self-learning cybersecurity solution would be "not at all useful", while 32% felt it would be "extremely useful."

The role of data science

Most cybersecurity professionals clearly believe that a blend of Artificial Intelligence, Machine Learning, and Deep Learning is vital in making inroads against cyber threats. The key to getting the best defenses is a case of *which* AI/ML/Deep Learning solutions to apply, rather than *whether* to incorporate AI/ML/Deep Learning at all.

of respondents agreed that "Data science (AI/ML/Deep Learning) can make a significant impact in preventing unknown threats and reducing false positives."

Conclusions & **Recommendations**

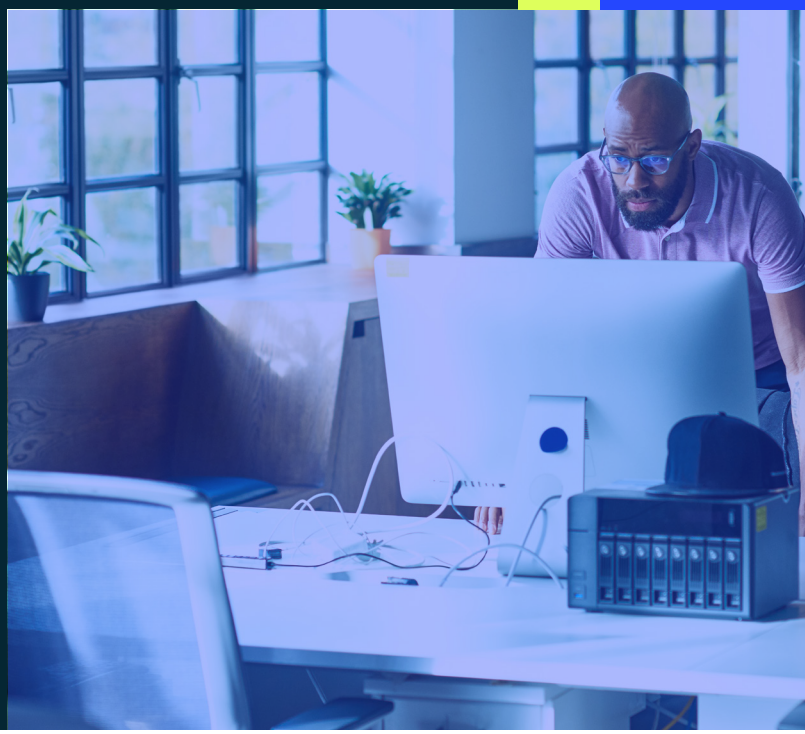
As of June 2021, the most prominent and public ransomware story was the Colonial Pipeline attack. By the time you read this, there will have been others – maybe more disruptive and costly to their target company or maybe with larger customer ramifications. Cyber threats are always going to pose a challenge to organizations, and yet most solutions currently available are not seen as optimal.

The research shows that there is clear evidence of widespread dissatisfaction of existing solutions among existing cybersecurity practitioners:

- The rate of change of the threat horizon is seen as exponential – infosec practitioners acknowledge it's getting harder to keep up and to prepare for more sophisticated threats
- Existing solutions, while largely adequate are not optimal for most users
- Practitioners are aware of the need for multi-vendor solutions to fully protect themselves against incursion
- Whilst ransomware is a key threat currently, it is not the only one keeping CISOs awake at night - prevention of zero day attacks is also a key concern
- Relatively few practitioners consider their EDR solution entirely optimal
- Managing false positives is a significant drain on a CISO's resources; Roughly a quarter of their team's time (and their own) is spent dealing with them
- There's also considerable evidence of concern over staff fatigue with the sheer volume of false positives
- Patches are seen as time consuming
- Automation is viewed by many as a central part of the solution

We conclude that in the eyes of the 600 cybersecurity professionals we spoke to, their "ideal" solution would integrate the following features:

- Primed to prevent zero day attacks
- Elimination of false positives
- Ransomware prevention guarantee
- Minimal patching, if any
- Minimization of impact on operating systems
- Easy integration with existing tools
- Highly automated solution
- Self-learning intelligent AI that is demonstrably effective in separating the threat signal from the false-positive noise
- Cost of implementation more than offset by cost savings in the SOC via false positive elimination



Appendix

Research methodology

Deep Instinct commissioned research on the threats faced by the cybersecurity community from independent marketing & market research company Hayhurst Consultancy in April / May 2021.

The Hayhurst Consultancy used their experience to examine the views of 600 cybersecurity professionals on the threats they face and the efficacy of the existing tools they use to combat those threats.

All surveys were conducted under the Market Research Society Code of Conduct using an online data collection approach supplemented by telephone-based research as required.

Respondent base

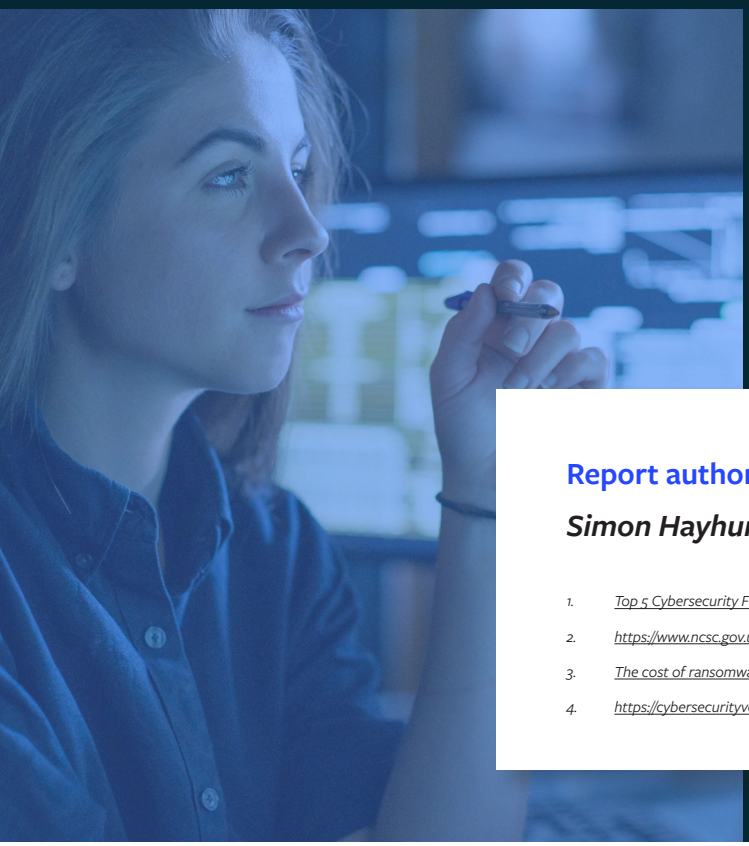
Interviews were conducted with 600 senior cybersecurity subject matter experts from companies in the U.S. (200), Canada (100), UK (100), Germany (100), and France (100).

All interviewees worked for businesses with 1,000 employees or more, and for businesses turning over at least US $500m annually.

Interviewees came from a broadly representative sample of businesses in Education, Financial Services, Manufacturing, Pharmaceuticals, Professional Services & Advisory, Retail, Technology, Telecoms, and Utilities.

Typical job roles of interviewees were CISO, CTO, ITO, Chief Security Officer, Head of Information Security, Information & Security Risk Manager, Malware Analyst etc.

All respondents were screened for having some level of input into the management of information security in their company. Almost half of respondents were the key decision maker in their organization with regards to information security.



Report author

Simon Hayhurst | *Director* | *The Hayhurst Consultancy*

1. *Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2020 To 2021 (cybersecurityventures.com)*
2. *https://www.ncsc.gov.uk/files/Annual-Review-2020.pdf page 83*
3. *The cost of ransomware attacks worldwide will go beyond $265 billion in the next decade | ZDNet*
4. *https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/*