TANIUM

Cybersecurity: Prevention is better than the cure

Foreword

Will 2022 be the worst year on record for cybersecurity? More than two-thirds (69 percent) of IT professionals certainly think so.

Behind this gloomy statistic, there are reasons to be optimistic about organisations' ability to cope with the evolving threat landscape. To empower IT and security teams with contextual, cross-industry data, Tanium commissioned a research project called 'Cybersecurity: Prevention is Better Than The Cure,' the findings of which are revealed here.

Do security teams have the strategic and financial support from senior management to tackle the unprecedented growth in attacks? Is security spending expected to increase over the next 12 months? Which sectors are most proactive and reactive when it comes to cyber? Read on to understand what's in store for the remainder of 2022.

Has the horse bolted?

Many security practitioners we heard from feel their work is ignored or undermined until it's too late. In fact, the research is quite conclusive that IT and security teams believe a cyber event has to occur before they can receive higher cybersecurity investments. Almost two-thirds of respondents (65 percent) agree, which sets a foundational question at the heart of the report: Is 2022 turning into a perfect storm for cybersecurity?

A common feature of large and growing organisations is the value they place on being faster and more agile. Resilience, on the other hand, is a less glamorous quality – one that often floats under the radar until it's needed. Eight in 10 (79 percent) professionals we surveyed said that more cybersecurity budget would likely be assigned following a data breach, not ahead of one. This is an acknowledgment that some senior leaders don't fully appreciate the preventative role that cybersecurity plays in protecting the business.

Lack of proactive investment can cause problems when it comes to preventing security incidents and data breaches. Over two-thirds (71 percent) of our survey sample claim to have a "preventative" approach to cybersecurity, yet three-quarters (76 percent) have suffered an attack that was "avoidable," begging the question: what types of preventative investments are being made?

These statistics highlight that there is ample scope for cyber teams to make improvements in many areas that are under their influence and control. As an illustration, almost half of the organisations surveyed (43 percent) said they intend to invest more in "employee awareness training." This prevention-first approach is one way to reduce vulnerabilities that are often caused by human error or lack of education on cyber matters.

Sector breakdown:

- Most preventative: **private healthcare sector with 88% claiming to have a mainly preventative approach to cybersecurity**
- Most reactive: **50% of state education institutions admit to being mainly reactive**
- Delayed funding: **manufacturing, with 80% saying that incidents need to happen before additional money is available**

"The cost of overcoming avoidable cyberattacks is where businesses really need to focus their attention and resource. Vulnerabilities occur where there are gaps in understanding and compliance across an organisation. Without a prevention-first approach, security professionals' will be heavily restricted in their ability to keep on top of the growing threat landscape."

"It's common, for example, for an organisation not to know basic facts around how many endpoints even exist (devices connecting to the corporate network). The trend towards greater remote and hybrid working only exacerbates the problem by widening the attack surface across corporate networks."

Oliver Cronk
Chief IT Architect, EMEA, Tanium

Fear of the known

So far, we've determined that the threat landscape is approaching "worst year" levels of concern. We've also learned that organisations will 'find the money' for cybersecurity, but often only after a problem has occurred. But what specifically are organisations fearful of should the firewalls be breached? The answer is inconclusive with a broad spread of equally-weighted concerns – until, that is, we look deeper into the data.

The largest number of survey respondents (56 percent) speculate that "loss of productivity" would have the biggest post-breach impact, followed by "loss of clients and/or revenue" (52 percent). However, it's worth noting that these two answers have a mutual association – downtime. Following two years of pandemic disruption, organisations are naturally sensitive to anything that interferes with business as usual.

Other listed concerns include: "financial damage from ransom payments" (49 percent), "reputational damage" (48 percent), "staff hours to recover from the incident" (47 percent) and "loss of IP/data" (46 percent). These answers are all the more interesting when we ask our respondents what they think concerns their senior leaders. Again, we get a fairly even spread of results, but with one significant discrepancy: just 36 percent believe that the "loss of intellectual property or owned data" would raise significant alarm in the boardroom.

Given these potential issues, it's not surprising that IT security professionals feel overstretched and underfunded. More than half (55 percent) believe they don't have enough staff to "focus sufficiently on cybersecurity preventative measures."

Ultimately, however, there is a strong feeling that prevention is better than the cure. 81 percent believe that more spending on preventative measures to stop cyberattacks and data breaches would "minimise" the impact of "avoidable incidents."

Sector breakdown:

- **Most concerned by productivity impact: telecoms (100 percent), private healthcare (88 percent)**
- **Least worried about IP/data loss: just 26 percent of public services orgs – excluding NHS and education – stated this concern**
- **Most under-staffed on cybersecurity: 83 percent of national health service respondents claim to be low on human resource**

"Attitudes towards cybersecurity vary between industries, just as they do within organisational hierarchies. Our data shows that the banking and university sectors are mostly concerned about the financial impact of a breach, whereas private healthcare, technology and telecoms firms are more worried about the loss of productivity during downtime. But what this shows is that IT and security teams are fully conversant with the main business-level concerns — they are not detached from them."

"This suggests that cyber teams need to redouble their efforts in educating senior executives about the merits of a prevention-first strategy – and to set investment levels appropriately. That's best achieved through contextual reporting of the threat landscape using insights that business leaders can interpret and act upon decisively."

Oliver Cronk
Chief IT Architect, EMEA Tanium

An under-policed crime wave

Returning to our headline statistic that this could be the worst year on record for cybersecurity, let's put some context around the claim. In 2021 alone, cyberattacks increased by 31 percent, including distributed denial of service (+11 percent) and phishing (+36 percent).* Looking ahead, is there anything to suggest an abatement of this worsening trend?

42 percent of businesses taking part in our research say they will spend more on new devices—which translates to more endpoints—over the next financial year. In contrast, just 18 percent forecast fewer devices (mobiles, laptops and printers) being added to the fleet of hardware joining company networks. Indeed, the telecoms industry – a leader in tech adoption – is clear about the trend toward device proliferation, with 75 percent anticipating more, not fewer, endpoints.

And if there's one thing we know, more endpoints generally requires more endpoint protection. With the exponential rise in remote working, it's not just company-owned devices connecting to the network that require protection. It's personal devices too. Technically, of course, these form part of the IT estate for cybersecurity purposes.

Consequently, three-quarters (75 percent) of professionals we surveyed said that they "carry a higher level of accountability" for cyberattacks and data breaches, compared to before the COVID-19 outbreak. Almost two-thirds (64 percent) also claim that their cybersecurity team is struggling to keep up with the volume and variety of cyberattacks. In truth, the burden of responsibility falls on the entire cybersecurity industry to come together and help organisations overcome these threats.

This leads us to an examination of the favoured tools and techniques of the cybersecurity function. Do these teams have the right toolboxes in place to tackle cyber threats and criminals effectively?

Sector breakdown:

- **Most concerned by productivity impact: telecoms (100 percent), private healthcare (88 percent)**
- **More endpoint protection: 60% of universities and manufacturers will invest more in endpoint security**
- **More responsibility for cybersecurity: IT and security professionals operating in manufacturing (83%), healthcare (83%) banking and finance (74%) have greater responsibilities since COVID-19 emerged**

"How are organisations' security teams expected to weed out the latent threats in their network and across distributed endpoints if they're not able to map their own estate? We believe security professionals when they say they have a preventative cyber strategy, but in truth, their net new funding is weighted more towards the remediation of breaches once they've happened. This is admitted, not denied."

"The scale and nature of cyberattacks demand that enterprises and the public sector become much more proactive in their approach. That starts with making sure your IT estate has a clean bill of health with zero compromised endpoints. By using lightweight, but fast and powerful asset discovery and inventory tools, IT and security teams can more easily identify what to keep and what to kill. Modernisation starts with visibility of your digital footprint and the controls in place to keep it clean."

Source: TechTarget (15 March 2022)

Final thoughts

Industry research is more interesting and useful when you examine the trends beneath the trends. What's clear is that cybersecurity is amidst a perfect storm. Industry data points to an expanding threat landscape with more sophisticated lines of attack and more persistent malicious activity. Threats are living longer in the network undetected before initialising their attacks.** Data loss and downtime are prevalent, which affects all lines of business – not just security teams.

Meanwhile, we have an exponential growth in devices – managed and unmanaged – being added to the IT estate that inevitably introduces new vulnerabilities. Cyber attackers can flourish under such conditions, particularly if there is more gateway access to data and less coordinated policing of the network.

In truth, most businesses have spent the last couple of years or more dealing with patched-up back-end infrastructure in order to keep the lights on and minimise the effects of the pandemic. They've accumulated too many disparate and poorly integrated front-end technologies in the process, making endpoint visibility and data integrity harder to maintain. At best, these are productivity drains; at worst, they're financial and reputational liabilities.

Against this backdrop of circumstances, it's easy to see why organisations feel that this could be the "worst year" for cybersecurity. But that's too simplistic, too reactionary, and altogether too pessimistic. Forward-thinking organisations will already be acting to pay down the technical debt of their legacy systems. 85% of security pros in our survey admit that "it costs more to recover from a cybersecurity incident than to prevent one." This much is understood.

The good news is that it doesn't necessarily require more tech and more spend to modernise cybersecurity performance. It can mean quite opposite - more rationalisation of the IT estate to lower the overall risk profile. That's an enticing proposition that can unite IT, security and business leaders around a common goal: prevention.

Source: "Ransomware attacks are on the rise and the criminals are winning"
New Scientist

Research recap

300 UK based survey participants from organisations with over 250 employees across banking, finance, education, healthcare, manufacturing, retail and telecoms. 23 percent have a C-suite and/or board-level role with 77 percent dedicated to IT and IT security.

Tanium offers an endpoint management and security platform built for the world's most demanding IT environments. Many of the world's largest and most sophisticated organizations — including nearly half of the Fortune 100, top retailers and financial institutions, and multiple branches of the U.S. Armed Forces — rely on Tanium to make confident decisions, operate efficiently, and remain resilient against disruption.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.