baesystems.com/financialservices

The COVID Crime Index 2021

Online, opportunistic and over-powering

BAE SYSTEMS

With 75% of banks and insurers experiencing cyber crime losses due to pandemic-related crimes, BAE Systems Applied Intelligence looks at how pandemic-related fraud and cyber crime are delivering a new blow to financial institutions.

Introduction

The pandemic that emerged globally in 2020 has impacted the world in ways never thought possible. It has changed behaviour both amongst businesses and communities, and fundamentally shifted how we live. The 'stay at home' order has been widespread and changed our daily routines, the way we work and has had a significant impact on the economy. Trillions has been lost globally.

However, although this change in lifestyle has had a positive impact on physical crime across the world – with numbers diminishing significantly – the changing conditions of business have driven an opportunistic uplift in online crime and fraud.

The BAE Systems Applied Intelligence COVID Crime Index 2021 report takes readers through a summary of the key challenges or factors that have hindered or impacted financial institutions (FIs) and their customers over the last 12 months. It provides global data and insights from IT security, risk and fraud teams, along with commentary and recommendations from BAE Systems Applied Intelligence experts, which we have provided a key summary of below.

COVID-19 has ushered in a new era of cyber crime and online fraud for Financial Institutions

74%

of FIs surveyed experienced a rise in malicious activity since the start of the pandemic. Of those, the average increase in criminal activity they detected was 29%

51%

were forced to adapt their security strategies as a result of the shift to distributed working — taking an average of 18 weeks to do so

74%

are concerned about the rise in pandemic-related cyber crime and fraud over the past year. Even more (77%) are worried about the anticipated rise in such threats over the coming year

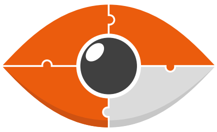
FIs budget cuts bite as cyber crime soars

IT security, cyber crime, fraud and risk funding has been cut by 26% on average over the past 12 months

Interestingly, that's almost exactly the same amount that detected criminal activity had risen by (29%) since the start of the pandemic

Reduced security budgets ultimately impact an FI's ability to protect IT systems and customers, driving further financial losses. In fact, over half have already seen a rise in losses over the past year

Consumers demand more from FIs



Nearly three-quarters of consumers have personally noticed an increase in fraudulent, cyber criminal or suspicious activity over the past 12 months. Nearly a quarter are now more concerned about cyber crime than they are physical crime

Half have been victims of cyber crime or online fraud in the past, a fifth over the past year. The average amount lost per individual was $1,179 (if refunded) or $746 (non-refunded) in both the UK and US

A quarter believe their FI could do a lot more to protect them from cyber crime and over half now think it's the job of FIs to do so — more so than the government, the police or themselves

Foreword

Dr Adrian Nish, Head of Cyber at BAE Systems Applied Intelligence

COVID-19 is a once-in-a-generation event that has defined the way we live and work in the 21st century. A global financial and health crisis in one, it demanded rapid and radical changes from businesses and consumers alike. Fortunately, most responded with determination and imagination to steer the ship safely through stormy seas.

Without wishing to understate the sacrifices many have made over the past year, the truth is that digital technology has saved the world from something that could have been even worse. According to McKinsey, the crisis "pushed companies over the technology tipping point", accelerating digitisation by years in some cases.[1] Consumers flooded online as physical retail stores closed, governments rapidly designed and delivered new digital services for furloughed workers and the unemployed, and organisations everywhere rushed to support remote working.

FIs, including banks and insurers, were no different. Over a third (35 per cent) of US customers are said to have increased their online banking usage during lockdown.[2] And more than 40 per cent of consumers across France, Germany and the UK say the way they bank has changed due to the crisis.[3] At the same time, IT departments also had to react rapidly to support an unprecedented switch to mass home working.

However, events of this magnitude also invite criminal activity. Fraudsters and cyber criminals are masters at exploiting fear, uncertainty and change to probe for weaknesses they can monetise. COVID-19 was no different. The bad guys reacted fastest and fiercest, adapting phishing campaigns, hunting out remote working security gaps, and preying on the vulnerable. We saw the number of ransomware victims more than double year-on-year and new techniques emerging. For example, at the start of 2020, only one ransomware operator was using the 'double extortion' technique, whereas now there are over 15 known groups performing such ransomware attacks – where criminals can increase their chance of making a profit by offering their victims an additional incentive to pay the ransom.[4] At the same time, budget cuts and new working patterns began to restrict the ability of IT security teams to mitigate these rising risks, cyber crime and fraud escalated.

Many argue that the pandemic may prove to be a tipping point for society.[5] If that is true, then there's much here to learn about the security and fraud challenges facing FIs and their customers. Our hope is that readers will use the insights we offer in these pages to build back stronger and better as the pandemic finally recedes.

Methodology

BAE Systems Applied Intelligence commissioned two surveys: one of 902 financial services organisations (referred to hereafter as FIs), and one of 2,003 consumers. These were carried out in both the US and UK markets by Atomik Research, an independent creative market research agency that employs MRS-certified researchers and abides to MRS code. The research fieldwork took place March 3 – 10, 2021.

[1] How COVID-19 has pushed companies over the technology tipping point
McKinsey (5 October 2020)

[2] Digital banking is surging during the pandemic. Will it last?
Penny Crosman, American Banker (27 April 2020)

[3] How COVID-19 could change the way we bank in Europe
Nigel Moden, EY (15 July 2020)

[4] 2020 Victim Analysis: BAE Systems Applied Intelligence

[5] Coronavirus: How the world of work may change forever
BBC (accessed 19 March 2021)

Chapter One

COVID-19 has ushered in a new era of cyber crime and online fraud for FIs

From the earliest months of the pandemic, most organisations saw attacks increase, as threat actors sought to capitalise on stretched IT teams, changing business priorities, and mass remote working. How effectively FIs were able to react to this new reality of doing business, and how much resource they put into threat prevention, may have had a significant impact on risk exposure and customer experience.

Worryingly, a large majority (77 per cent) of FI respondents remain concerned about these same trends continuing to drive up fraud and cyber crime over the coming year.

COVID spurs cyber crime

It's abundantly clear the pandemic led to a surge in cyber crime and fraud against global FIs. Nearly three-quarters (74 per cent) of those we spoke to said they'd experienced a rise in malicious activity since the start of the crisis. Of those, the average increase in criminal activity detected was 29 per cent.

When asked for more detail, respondents pointed to a wide range of threat activity, most notably mobile malware, phishing, botnet attacks, ransomware and new COVID-related malware, as well as insider threats. Phishing is often the initial vector via which other threats, like ransomware and mobile malware, are spread. It remains a popular method of attack, because it successfully exploits the perceived weakest link in an organisation's security posture: its employees.

The pandemic has further exposed potential corporate security weaknesses. Over half (59 per cent) of respondents said they thought non-IT staff are more at risk of falling for phishing scams when working from home, because they're unable to ask for advice as easily.

It's worth remembering, however, that despite COVID-19 giving cyber criminals a highly effective lure for reeling in phishing victims, rates of COVID-themed scam emails weren't as high as expected. Microsoft claimed in April 2020 that less than 2 per cent of the total volume of email-borne threats it tracked daily had COVID-related attachments or URLs.[6] In reality, cyber criminals are likely to have rebranded existing campaigns with COVID-19 themes and lures rather than expanded their wholesale efforts, although this shouldn't downplay the risk to organisations. With phishing, just one misplaced click by an employee could lead to a major security breach.

> "The pandemic has offered cyber criminals and fraudsters new opportunities to probe for weaknesses they can monetise and new ways to disguise their activity."

Dr Adrian Nish
Head of Cyber
BAE Systems Applied Intelligence

The mass shift to remote working

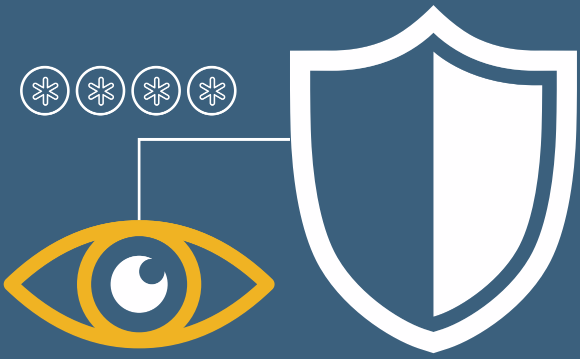
The mass shift to remote working had a major impact on corporate cyber risk, making it harder for security teams to work effectively and expanding FIs' cyber perimeter. Over half (51 per cent) of businesses surveyed claimed they were forced to adapt their security strategies as a result of the shift to distributed working — taking an average of 18 weeks to do so.

This is valuable time during which attackers may have had an advantage in exploiting gaps in protection. But despite this, our research shows 14 per cent of respondents said they are still evolving their capabilities. And over a quarter (27 per cent) claimed the pivot to remote working did not accelerate their adoption of cloud security measures. This is a cause for concern, given that the adoption of new digital technologies can provide new opportunities for attackers, if not properly protected, for example, in exploiting unpatched vulnerabilities in Software as a Service (SaaS) applications or misconfigured cloud infrastructure.

The shift to remote working also created countless newly distributed endpoints for IT security teams to manage and patch, together with remote access infrastructures unable to cope with the surge in demand. Many virtual private networks (VPNs) were quickly overwhelmed, leaving remote workers even more exposed. One report claimed two-fifths (38 per cent) of global IT leaders are reducing their reliance on VPNs as a result, and that 43 per cent had problems patching personal devices.[7] Ransomware threat actors were observed ramping-up attacks to exploit VPN vulnerabilities and network gateway appliances to compromise organisations.[8] The remote desktop protocol (RDP) used to facilitate remote working was also exploited by attackers, who breached credentials with ease on the dark web.[9] As a result, ransomware became the number one vector last year.

In total, the vast majority (86 per cent) of FI respondents admitted the initial mass move to remote working made their organisation less secure, with 44 per cent complaining of a lack of visibility into their networks. A significant minority (14 per cent) also claimed that the productivity of IT security teams declined when forced to work from home. That's not to mention the potential impact of home working on regular employees. Research has revealed that cyber hygiene and best practice is often ignored by staff working away from the office.[10] Users may be more distracted at home, and their devices and networks may not be as secure. All of this creates the perfect conditions for cyber criminals and fraudsters to exploit.

Research has revealed that cyber hygiene and best practice is often ignored by staff working away from the office



It's clear that FIs need a more effective and efficient way to assess and manage cyber risk

Concerns continue

As a result, three-quarters (74 per cent) of FI respondents said they were concerned about the rise in pandemic-related cyber crime and fraud over the past year. More concerning still is that a fifth (19 per cent) said they weren't confident in their organisation's ability to protect their customers in 2020, while a similar number (17 per cent) have little confidence in their efforts to block cyber threats and fraud in 2021. And looking to the future, 77 per cent were worried about the anticipated rise in such threats over the coming year.

Going forward, it's clear that FIs need a more effective and efficient way to assess and manage cyber risk. When it comes to ransomware, for example, the focus should be on best practices such as secure back-ups, regular patching, perimeter protection and network segmentation.[11] Failure to do so could not only lead to major security breaches, resulting in financial and reputational damage, but also to loss of customer confidence.

75%

of FI respondents have experienced cyber crime losses due to pandemic-related crimes

77%

are worried about the continued rise in such threats over the coming year

86%

of FIs admitted the initial mass move to remote working made their organisation less secure

The impact of COVID-19 meant that almost one-fifth (19%) of FIs weren't confident in their ability to protect their customers in 2020

35%

Increase in botnet attacks

35%

Rise in ransomware

35%

Rise in phishing attacks

32%

Increased mobile malware

30%

New Covid-related malware

29%

Uplift in insider threats from WFH

Chapter Two

Budget cuts bite as cyber crime soars

Money is at the heart of cyber crime, but it could also be part of the solution. Cyber criminals and fraudsters are the ultimate profit-driven adversaries. Everything they do is a cold calculation of ROI. If successful, their efforts can cause significant financial and reputational damage to the victim organisation. In this context, extra spending on cyber security budgets might seem like a no-brainer; however, in reality, we found that many organisations cut security spend due to the financial pressures of COVID-19.

The key to charting a responsible path forward is ensuring the organisation has sufficient funding to protect customer data and IT systems. But it must also be spent wisely, staffing and technology can have the biggest positive impact on risk levels. These discussions could have a profound impact on FIs success as they seek to emerge from the pandemic in a strong position.

Budgets slashed

Our survey found IT security, cyber crime, fraud and risk funding has been cut by 26 per cent on average over the past 12 months. Interestingly, that's almost exactly the same amount that detected criminal activity had risen by (29 per cent) since the start of the pandemic. Short-term financial decisions are often made without full appreciation of the potential long-term effects. Thus, although many FIs cut funding in the face of significant economic headwinds,[12] there could be a major cost to this going forward.

In fact, 40 per cent of respondents told us that critical IT security technology spend may have to be cut as a result of budget cuts and a similar number (39 per cent) said they will be unable to action their entire cyber security strategy. Respondents also warned that customers would be put at greater risk of cyber crime or fraud (37 per cent), and that they may be hit by the double whammy of losing experienced security professionals (36 per cent) without being able to make essential new hires (29 per cent).

The key to charting a responsible path forward is ensuring the organisation has sufficient funding to protect customer data and IT systems.

Counting the cost of cyber attacks

Reduced security budgets ultimately impact an FI's ability to protect IT systems and customers, driving further financial losses. In fact, over half (55 per cent) of respondents said they'd already seen a significant (16 per cent) or slight (39 per cent) rise in losses over the past year. On average, they believed that cyber crime and/or fraud had cost their business approximately $720,000 over that time.

No two organisations or cyber incidents are the same, and some estimates put the figure even higher — at $3.9 million per data breach.[13] Typical losses could include:

- **IT overtime** for incident response, remediation and clean-up
- **Ransomware payments** — the average in Q4 2020 was around $154,000 (£111,000)[14]
- **Operational outages** — a leading US healthcare provider claimed it would suffer $67 million (£48m) in losses due in part to losing custom to rival providers during a ransomware attack[15]
- **Legal costs** following a major breach, especially if a class action lawsuit is filed
- **Customer churn,** with associated financial costs

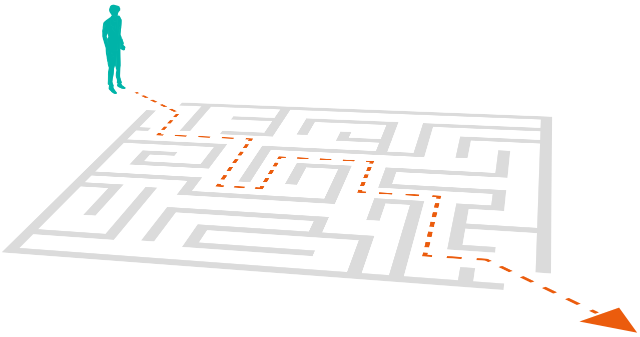
The vast majority (75 per cent) of FI respondents claimed the cyber crime losses experienced by their business over the past year were due to pandemic-related crimes. As discussed in the last chapter, these range from ransomware and mobile malware to bot-powered attacks, COVID-related malware and even insider attacks. Such attacks are now easier for threat actors to monetise thanks to the opportunities afforded them by the mass move to remote working — distracted home workers, exposed IT infrastructure, reduced IT and security budgets, and IT security teams unable to gain adequate network visibility.

Humans vs. humans

Cyber security, like cyber crime, is ultimately a human-shaped challenge. Technology is merely a tool and platform for attacks — people launch them, and people protect organisations against them. It's of some concern, therefore, that many (36 per cent) respondents felt that budget cuts could mean losing key staff members. But, in fact, we found that slightly more (36 per cent) FIs hired new security professionals during the pandemic than were forced to let them go (28 per cent).

The sheer rise in threats should tell us what's at stake here. Organisations made significant additional cloud and digital infrastructure investments during the pandemic, which would have needed extra resource to be managed securely. Global cloud spending rose 37 per cent year-on-year in the first quarter of 2020, for example.[16] These extra pressures may have left many under-staffed IT teams struggling to manage new priorities, therefore impacting their ability to keep the organisation secure.

Greater productivity could be achieved without increasing headcount. There's no value in hiring new security operations centre (SOC) analysts if they are using a disjointed set of tools which fails to prioritise threat alerts for them, for example. A focus on automation, tool consolidation and machine learning-powered threat detection and response technology could make a major positive impact here.



Emerging from the pandemic

The impact of the pandemic on future growth is also a concern for FIs. Over a quarter of respondents said COVID-19 has delayed their move to the cloud (28 per cent), and reduced R&D budget (25 per cent) and innovation (24 per cent). However, there are some reassuring signs that the extreme measures forced upon FIs over the past year hopefully won't be the norm going forward.

For many businesses, the world will not return to 'normal' for some time, and adjustments will potentially need to be made for the long term. Following the release of the UK Government's lockdown exit roadmap, nearly half (42 per cent) of UK respondents claimed tech and R&D spending (39 per cent) is on the rise. Others spoke of budget cuts being put on hold (38 per cent) and hiring reinstated (39 per cent). This bodes well for the sector's recovery over the next 12 months, as long as funding is directed to the areas that need it most.

The impact of COVID-induced budget cuts to FIs

40% may need to cut back on IT security technology spend

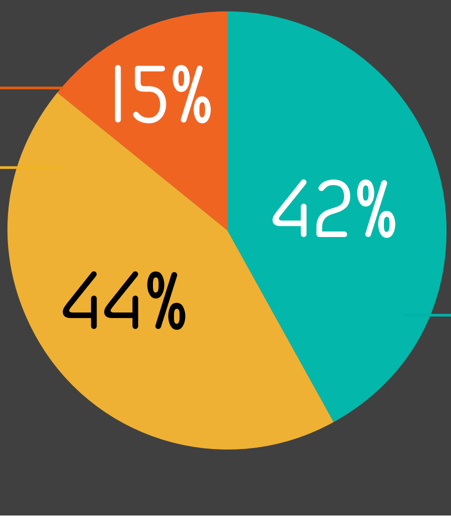
39% will be unable to fulfil all the parts of their cyber security strategy

36% risk losing experienced security professionals

29% won't be able to make essential new hires

IT security funding has been cut by 26% on average over the past 12 months

almost exactly the same amount that detected criminal activity had risen by (29%) since the start of the pandemic



15% of FIs said it had little or no impact

42% of FIs have been made less secure by remote working model due to COVID-19

44% of FIs said they have less visibility of holes in their network or infrastructure

Chapter Three

Consumers demand more from their FIs

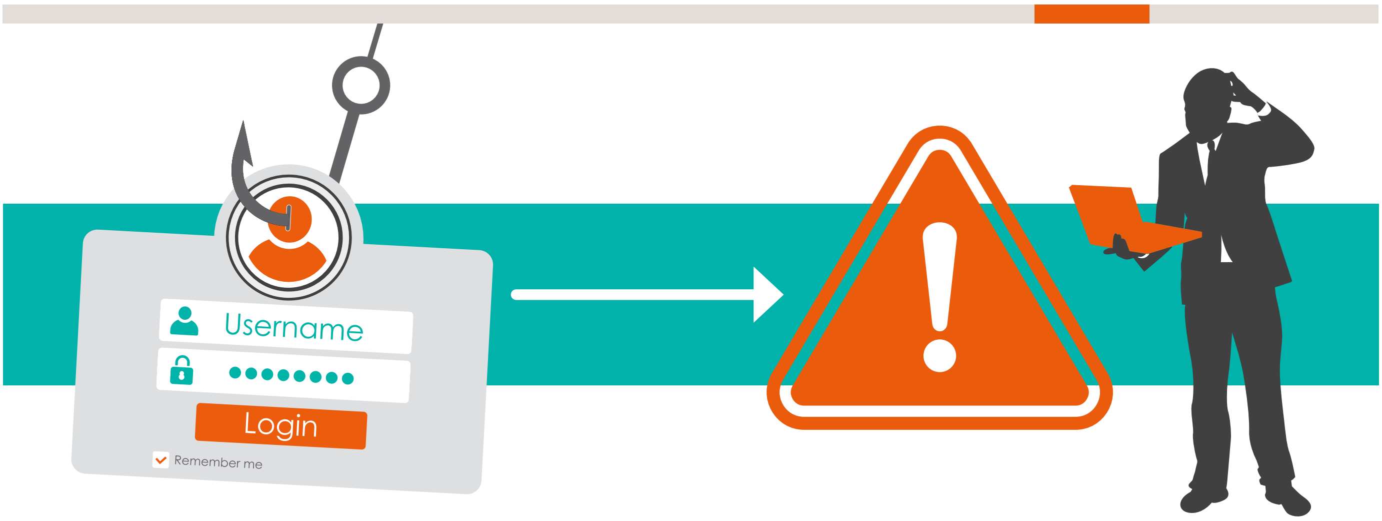
As useful as it is to understand corporate cyber risk from an internal perspective, it's also important to look at the customer experience of online threats. That's because changes in consumer behaviour, and the perceived role FIs should play in preventing cyber crime and fraud, both influence customer loyalty. Our research found that as consumers raced to online shopping during the pandemic, more were exposed to financial fraud and cyber attacks. This, in turn, has driven both awareness levels and expectations of FIs regarding how to combat such crimes.

There are opportunities here for FIs to differentiate by providing enhanced education and support, alongside back-end fraud screening and world-class cyber security to attract new customers.

Online is the new normal

The pandemic unsurprisingly drove a huge surge in online activity. Only 8 per cent of respondents claimed that they try to avoid e-commerce, with 36 per cent claiming they do all their shopping online now, and a further 33 per cent said their online purchasing had increased. Some 15 per cent said they hadn't shopped at all online pre-pandemic, but now do so regularly. This highlights a huge change of consumer behaviour for FIs to grapple with.

However, these trends have also exposed consumers to a greater risk of scams and cyber threats. Over a quarter (26 per cent) of those we spoke to said they'd bought something from a fraudulent site over the past year. Separately, more than three-quarters (78 per cent) are now concerned about the need to share personal information with e-commerce sites.



Opportunity knocks for cyber crime

Where and how often does online crime happen? Half (50 per cent) of consumers we spoke to have been victims of cyber crime or online fraud in the past, and a fifth (19 per cent) over the past year. Yet, while nearly two-fifths (38 per cent) of these victims said it happened just once, a quarter (24 per cent) claimed it happened twice in a year and 15 per cent three times. This is a troubling statistic indicating consumers are failing to adopt safer online behaviour, or that the scammers are getting better at tricking them.

The most common cyber incidents were phishing (83 per cent), bank or credit card fraud (78 per cent), stolen data (70 per cent), hoax SMS messages (78 per cent), hoax phone calls (79 per cent) and ransomware (55 per cent). In addition, more than a quarter of consumers (28 per cent) said they'd received an email scam relating to COVID-19 and 22 per cent via SMS. In fact, phishing emails, SMS messages and scam phone calls are all variations on the same theme — a fraudster impersonating a legitimate organisation in order to deploy malware, or trick the respondent into handing over personal and financial details. This information is then typically used in follow-on fraud, such as card payments made in the victim's name.

Such threats can be extremely stressful for those affected, especially during a time of financial crisis and tremendous uncertainty over jobs. We found the average amount lost through these incidents was $1,179 (if refunded) or $746 (non-refunded) per individual in the UK and US.

Where the buck stops

The impact of surging online attacks has seen increased consumer awareness. Nearly three-quarters (72 per cent) told us they have personally noticed an increase in fraudulent, cyber criminal or suspicious activity over the past 12 months. Nearly a quarter (23 per cent) are now more concerned about cyber crime than they are physical crime.

There are a couple of further knock-on effects to note here. Firstly, there's a growing concern over sharing personal information via digital channels. 84 per cent said they were worried about sharing digital identity data online, and just under a third (31 per cent) claimed they don't feel safe about how much they've had to share online during the pandemic. This could be viewed positively, as consumers becoming more "digital-savvy" and therefore less likely to fall for scams, although the data above would seem to contradict that. On the other hand, if consumers lose trust in the security of digital channels in general, it could spell bad news for FIs hoping to streamline processes and trim costs by pushing more services online.

Consumers are now also demanding more support from FIs to help keep them safe online. A quarter (24 per cent) of respondents believe their FI could do a lot more to protect them from cyber crime and over half (53 per cent) now think it's the job of FIs to do so — more so than the government (47 per cent), the police (34 per cent) or themselves (40 per cent).

A chance to shine

Overall, 30 per cent of consumers believe there's not enough guidance on who to report online crimes to. More than half (56 per cent) also want greater transparency from their FIs about cyber crime levels, more guidance (53 per cent) on how to behave online and more educational content (47 per cent). A further 55 per cent said they actively consider cyber crime protection when choosing a bank or card provider, and significantly more (84 per cent) claimed that if changing providers, they'd now consider how proactive the provider is with cyber crime protection.

These findings represent a clear opportunity for FIs to embrace education and customer outreach as key differentiators, as well as back-end fraud prevention and cyber security. It's clear that FIs must not only enhance corporate cyber security and fraud protection, but also accessibly communicate these improvements to reassure customers, and share advice on how to stay safe online. This would not only help drive customer loyalty, but also reduce cyber crime-related losses.

On the plus side, only a small percentage (10 per cent) of the consumers we spoke to are not confident in their FIs ability to protect them. The industry should build on these strong foundations of trust to drive success going forward.

Consumer behaviour is changing

72%
of consumers have noticed an increase in fraudulent, cyber criminal or suspicious activity over the past 12 months

26%
of consumers bought something from a fraudulent site over the past year

84%
said they were worried about sharing identity data online

23%
are now more concerned about cyber crime than they are about physical crime

55%
of consumers now actively consider cyber crime protection when choosing a bank or card provider

56%
of consumers want greater transparency from their FIs about cyber crime levels

53%
want more guidance from FIs on how to behave online

47%
want more educational content from FIs

Conclusion

Navigating a post-pandemic world

The COVID-19 crisis has dramatically altered the operational and cyber risk landscape for FIs, leading to surging levels of cyber crime and fraud. Mobile malware, phishing, botnet attacks, ransomware, new COVID-related malware strains and insider threats have all increased, just as FIs' ability to mitigate these risks has decreased. The mass shift to remote working is partially responsible for both trends, creating more human and technology-related security gaps for criminals to exploit and operational challenges for IT security teams.

Many of the FIs surveyed feel less secure since the start of the pandemic, and this is in part due to budget cuts. In many cases, these have put key strategic efforts at risk and led to an increase cyber crime and fraud related losses, although there are positive signs from the UK that the successful vaccine roll-out has put such cuts on hold. That being said, these are clearly worrying times for FIs: a majority are concerned about the continued rise of cyber threats and fraud in 2021, and aren't confident in their ability to manage such risks.

Consumers have also suffered financially during the pandemic. Gravitating online during lockdowns, they've been exposed to surging levels of card fraud, data theft, phishing, ransomware and more. They're more concerned about cyber crime and fraud than ever before, and want their banks to do more about it — by providing additional guidance and education, and greater transparency around cyber crime levels. Despite this concerning picture, there is an opportunity for FIs to add value for these consumers and market differentiation by offering improved protection from cyber risks.

So how do they do that?

FIs must start by enhancing corporate cyber security. This begins with gaining visibility into risk — by methodically mapping all of their key assets and data flows, understanding the main threats and attack vectors facing their organisation, and where vulnerabilities and security gaps lie.

Next, FIs need to manage that risk. This comes down to three pillars: people, process and technology.

People are at the heart of the cyber security/fraud problem, but can also be a big part of the solution too. FIs should enhance employee training to create a stronger first line of defence, and break down legacy siloes between cyber crime, fraud and risk teams. They need to encourage more sharing of intelligence, both within organisations and across industry. The Intelligence Network, a BAE Systems Applied Intelligence initiative, already working to bring together like-minded professionals and influencers from across industry.

Process is also key. These are the day-to-day activities that drive better security and fraud protection, with prioritising assets, regular patching and vulnerability scanning, incident response and threat intelligence gathering. BAE Systems Applied Intelligence offers regular threat intelligence insights to inform your processes and enhance your ability to detect and respond rapidly to emerging threats.

Finally, there's **technology**: the tools and systems designed to run your security and fraud processes. Defence-in-depth protection could include security controls at the network, endpoint, server and gateway layers, and focus on automation and simplicity. Too many tools will quickly become unmanageable for stretched IT teams. BAE Systems Applied Intelligence offers experts advisory sessions for cyber security and fraud protection which could help to shape your technology strategy.

These are challenging times, but risk and opportunity are two sides of the same coin. The FIs likeliest to succeed as we exit the pandemic will be able to manage both to enhance their capabilities and reputation among customers.

BAE SYSTEMS

At BAE Systems, we provide some of the world's most advanced technology, defence, aerospace and security solutions.

We employ a skilled workforce of 87,800 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Appendix

[1] How COVID-19 has pushed companies over the technology tipping point
McKinsey (5 October 2020)

[2] Digital banking is surging during the pandemic. Will it last?
Penny Crosman, American Banker (27 April 2020)

[3] How COVID-19 could change the way we bank in Europe
Nigel Moden, EY (15 July 2020)

[4] 2020 Victim Analysis
BAE Systems Applied Intelligence

[5] Coronavirus: How the world of work may change forever
BBC (accessed 19 March 2021)

[6] Microsoft shares new threat intelligence, security guidance during global crisis
Rob Lefferts, Microsoft (8 April 2020)

[7] Security threats spiked when the world stayed home
Tanium (accessed 16 March 2021)

[8] Microsoft works with healthcare organizations to protect from popular ransomware during COVID-19 crisis: Here's what to do
Microsoft (1 April 2020)

[9] Ransomware Payments Up 33per cent As Maze and Sodinokibi Proliferate in Q1 2020
Coveware (29 April 2020)

[10] Employee Security Training is Vital to Remote Success
Trend Micro (21 June 2020)

[11] Ransomware: The Storm Continues
BAE Systems Applied Intelligence

[12] COVID-19: Impact on the banking sector
KPMG (accessed 16 March 2021)

[13] Cost of a Data Breach Report 2020
IBM Security (accessed 16 March 2021)

[14] Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands
Coveware (21 February 2021)

[15] Universal Health Services, Inc. Reports 2020 Fourth Quarter And Full Year Financial Results And 2021 Full Year Earnings Guidance
UHS (25 February 2021)

[16] Cloud providers see "aggressive" growth amidst Covid-19 pandemic
Alex Alley, Datacenter Dynamics (4 May 2020)

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
Level 1
14 Childers St
Canberra
ACT 2601
Australia
T: +61 1300 027 001

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/financialservices

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai