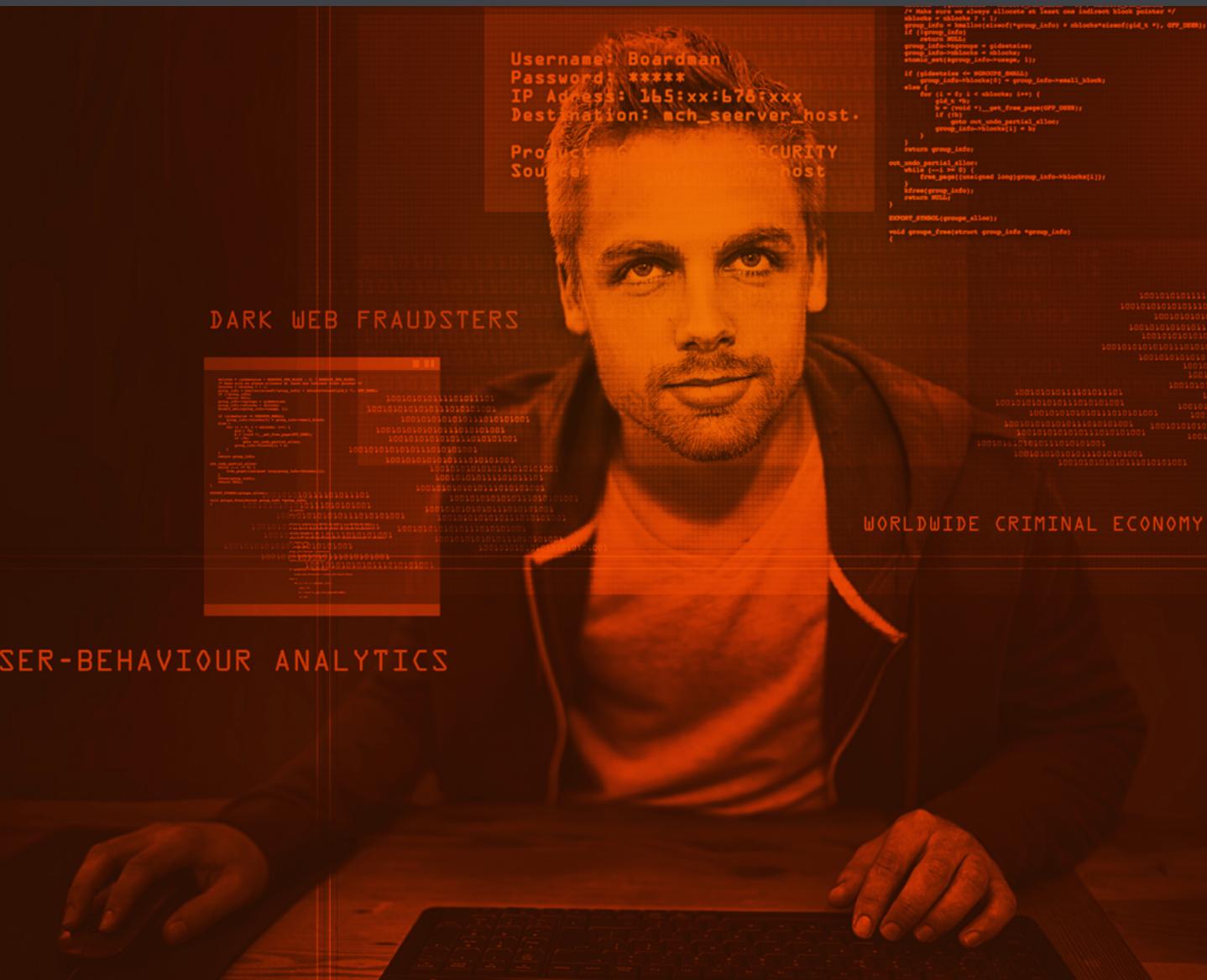


The fightback starts here

Future-proofing insurers against financial crime



Username: Boardman
Password: *****
IP Address: 165:xx:b76:xxx
Destination: mch_seerver_host.
Product: SECURITY
Source: host

```
/* Make sure we always allocate at least one (minimum block pointer) */
shlblock = shlblock + 1;
group_info = shlblock[shlblock * group_info + shlblock * sizeof(gid_t), GFP_KERNEL];
if (!group_info)
    return 0;
group_info->group = gidblock;
group_info->shlblock = shlblock;
shlblock_ptr[group_info->group, 1];
if (gidblock == 0)
    group_info->shlblock[1] = group_info->shlblock;
else {
    for (i = 0; i < shlblock; i++) {
        gid_t gid;
        if (gid == 0)
            gid = group_info->shlblock[i];
        if (gid)
            group_info->shlblock[i] = 0;
    }
    return group_info;
}
net_link_group_info:
while (link < 0) {
    link = group_info;
    return link;
}
EXPORT_SYMBOL(group_info);
void group_free(struct group_info *group_info)
```

DARK WEB FRAUDSTERS

```
1: group_info;
2: group_info;
3: group_info;
4: group_info;
5: group_info;
6: group_info;
7: group_info;
8: group_info;
9: group_info;
10: group_info;
11: group_info;
12: group_info;
13: group_info;
14: group_info;
15: group_info;
16: group_info;
17: group_info;
18: group_info;
19: group_info;
20: group_info;
21: group_info;
22: group_info;
23: group_info;
24: group_info;
25: group_info;
26: group_info;
27: group_info;
28: group_info;
29: group_info;
30: group_info;
31: group_info;
32: group_info;
33: group_info;
34: group_info;
35: group_info;
36: group_info;
37: group_info;
38: group_info;
39: group_info;
40: group_info;
41: group_info;
42: group_info;
43: group_info;
44: group_info;
45: group_info;
46: group_info;
47: group_info;
48: group_info;
49: group_info;
50: group_info;
51: group_info;
52: group_info;
53: group_info;
54: group_info;
55: group_info;
56: group_info;
57: group_info;
58: group_info;
59: group_info;
60: group_info;
61: group_info;
62: group_info;
63: group_info;
64: group_info;
65: group_info;
66: group_info;
67: group_info;
68: group_info;
69: group_info;
70: group_info;
71: group_info;
72: group_info;
73: group_info;
74: group_info;
75: group_info;
76: group_info;
77: group_info;
78: group_info;
79: group_info;
80: group_info;
81: group_info;
82: group_info;
83: group_info;
84: group_info;
85: group_info;
86: group_info;
87: group_info;
88: group_info;
89: group_info;
90: group_info;
91: group_info;
92: group_info;
93: group_info;
94: group_info;
95: group_info;
96: group_info;
97: group_info;
98: group_info;
99: group_info;
100: group_info;
```

WORLDWIDE CRIMINAL ECONOMY

USER-BEHAVIOUR ANALYTICS

■ Executive summary



Dennis Toomey,
Global head
insurance fraud
product manager,
BAE Systems

The criminal threats facing insurers are sophisticated, global and ever-growing. They are also difficult to identify and quantify with accuracy, making them hard to combat. But it is clear that the most successful companies of tomorrow will be those who put in the most work today to anticipate and negate future challenges.

The global cost of fraud across all sectors could be as much as £3.2 trillion per year, according to consultants Crowe¹. Meanwhile, Accenture² suggests that companies worldwide could incur \$5.2 trillion in costs and lost revenue from cyber attacks over the next five years.

Consistency and collaboration are essential. If insurers continue to tackle financial crime in a piecemeal fashion, without understanding the true scope and intricacy of the problem, they will be forever playing catch-up. So how can insurers, whose customer data makes them a prime target for criminals, future-proof themselves against these risks?

The solution, as well as the problem, often lies in the cultural, operational and data silos within which they operate, as this paper will explain.

¹ <https://www.crowe.com/uk/croweuk/insights/financial-cost-of-fraud-2018>

² <https://newsroom.accenture.com/news/cybercrime-could-cost-companies-us-5-2-trillion-over-next-five-years-according-to-new-research-from-accenture.htm>

£3.2
TRILLION
annual cost of
fraud globally

\$5.2
TRILLION
annual cost of
cyber attacks
globally

Quantifying a global problem

Insurance fraud is not a new phenomenon. Indeed, an epigram by the Roman poet Martial provides clear evidence of its existence in the Roman Empire during the first century AD:

“Tongilianus, you paid two hundred for your house;
An accident too common in this city destroyed it.
You collected ten times more. Doesn't it seem, I pray,
That you set fire to your own house, Tongilianus?”

Fraud and financial crime are ancient problems then, human instinct even.



\$80bn

The infographic consists of a large orange circle with a white dotted border. Inside the circle, the text "\$80bn" is written in a large, white, sans-serif font. Below the circle, there is a small world map graphic.

amount US Coalition Against Insurance Fraud estimates is lost annually to fraudulent claims⁵



86%

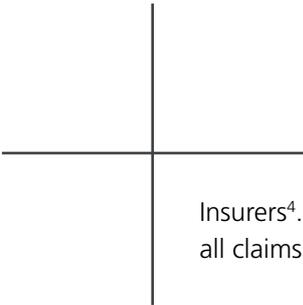
The infographic consists of a large white circle with a grey dotted border. Inside the circle, the text "86%" is written in a large, black, sans-serif font. Below the circle, there is a small world map graphic.

of financial services firms experienced a cyber attack in the last 12 months³

According to a 2017/18 Global Fraud & Risk Report by Kroll³, 84 per cent of financial services firms experienced fraud and 86 per cent experienced a cyber attack in the preceding 12 months, the highest rate reported by any sector.

And when we narrow the scope down, we see that the insurance industry is a particular target. Insurance companies in the UK identified over 500,000 cases of potential fraud, amounting to £1.3 billion, in 2017 says the Association of British

³ <https://www.kroll.com/en/insights/publications/global-fraud-and-risk-report-2018>



Insurers⁴. In the US, the Coalition Against Insurance Fraud⁵ estimates that 3-4 per cent of all claims are fraudulent, costing the industry around \$80 billion a year.

Clearly, the threat is significant and its geography diffuse, but the fightback is thwarted by a lack of precise and detailed information.

Nicholas Ryder, a professor in financial crime at the University of the West of England, says the situation is stark: “Financial institutions lack the overall view of the threat. I generally think corporations are pretty much in the dark over some of the threats posed by financial crime.”

Problems created by this incomplete picture are exacerbated by the industry’s traditional reluctance to share data. Such barriers – both within the industry and across national borders – are in stark contrast to the methods used by criminal gangs.

“Much of the criminal threat facing organisations is transnational,” says Professor Ryder. “Criminals are making huge sums of money.” The fact that these gains are often funnelled into other criminal enterprises gives a broader, societal dimension to the industry’s response to crime.

The enemy: an international criminal network

There is evidence that organised crime gangs are working together across borders to perpetrate insurance fraud.

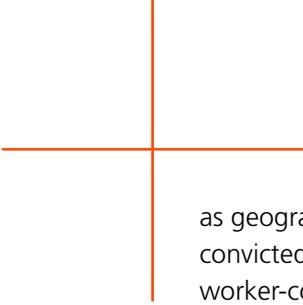
In one case, Colombian drugs traffickers laundered \$80 million through life-insurance policies issued in – of all places – the Isle of Man⁶. In another, members of a crime ring

⁴ <https://www.abi.org.uk/news/news-articles/2018/08/one-scam-every-minute/>

⁵ <https://www.heraldtribune.com/news/20021207/feds-say-traffickers-used-insurance-to-launder-80m>

⁶ <https://www.heraldtribune.com/news/20021207/feds-say-traffickers-used-insurance-to-launder-80m>





as geographically far-flung as Iran, Germany, the Philippines, Mexico and Armenia were convicted in 2011 for defrauding 70 US insurers of more than \$11 million through false worker-compensation claims⁷.

Criminals are increasingly finding sophisticated ways to deploy each others' networks and skill sets for mutual profit in a worldwide criminal economy. The bad guys, it seems, are already collaborating.

Pooling knowledge, breaking the under-reporting habit

Working together is key to the fightback. Effective public-private partnerships, which share information and data on financial crime, are an essential element of insurers' efforts to defeat the criminals, protecting themselves and the industry for the future.

"Criminals are increasingly finding sophisticated ways to deploy each others' networks and skill sets for mutual profit in a worldwide criminal economy"

Dennis Toomey

Without this, Professor Ryder believes financial institutions will continue to struggle against the growing criminal threat because "under-reporting of criminal incidents inhibits the ability to understand how big the problem is".

The extent of this problem and the need for cross-sector partnership is clear. Only 54 per cent of IT security departments did, or would, report a ransomware attack to law enforcement, with only 61 per cent even willing to report an incident to their own board, it was reported in a 2016 global survey⁸ by IT security firm SentinelOne.

The situation with fraud specifically is more reassuring, with progress made in the UK through the establishment of the Insurance Fraud Bureau. This acts as a central fraud-data resource and provides operational support.

In the US, the Coalition Against Insurance Fraud has lobbied successfully over the years for tougher legislation to fight this kind of crime and raise awareness of the problem.

Equivalent bodies to tackle the cyber threat are less advanced. With the connections between cyber crime and fraud ever stronger, many observers argue that this data gap could hamper the fight against fraud as well as against cyber crime.

Efforts are under way to change that. The Intelligence Network⁹, launched by BAE

⁷ <http://www.insurancefraud.org/article.htm?RecID=3350>

⁸ <https://go.sentinelone.com/rs/327-MNM-087/images/SentinelOne-Global.pdf>

⁹ <https://content.baesystems.com/theintelligencenetwork/uk>

“With the dark web fraudsters can take what they used to do in the open so much further”

Dennis Toomey



Systems in July 2018, is one example of a working community of cyber and financial crime professionals collaborating to understand and tackle cyber security issues. Member organisations include telecoms operators and the UK National Cyber Security Centre (NCSC).

Networks of agencies working to support private enterprise against cyber attacks are a good starting point. Mark Brenlund, partner at UK law firm Weightmans, explains: “This is a combination of people, process and technology.” Private industries gain intelligence – ‘knowledge which they monetise’ – by engaging covertly with hackers on the dark web to understand what they are doing and then build appropriate defences.

Transparency is intrinsically problematic in this field. “They will engage with the National Crime Agency (NCA) and the NCSC, but if the information is spread widely across the industry, it could alert hackers that covert operations are under way and lead them to stop talking to the operatives,” says Brenlund.

To view this as purely a problem for the cyber security community is to misunderstand the nature of the problem evidenced in the shadier corners of the web.

For example, cyber security firm Trustwave¹⁰ has discovered that cyber criminals are advertising ‘jobs’ for individuals willing to take part in insurance fraud, specifically crash for cash.

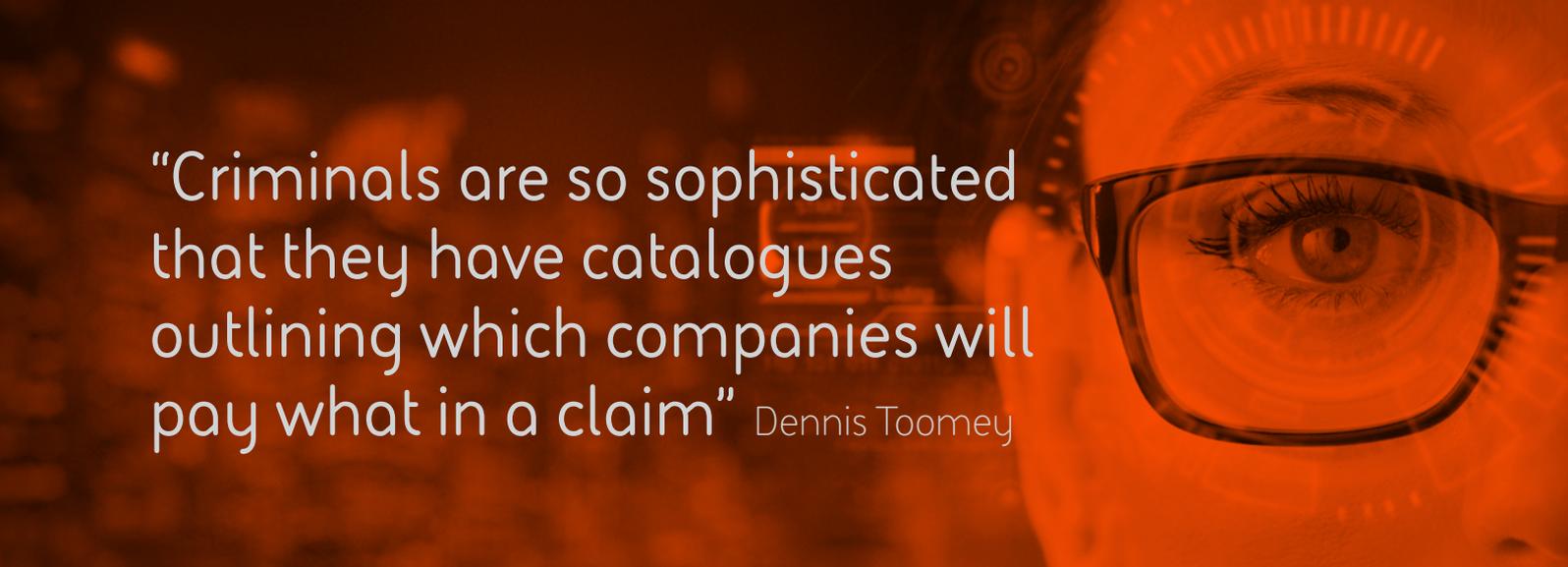
“With the dark web fraudsters can take what they used to do in the open so much further,” says Dennis Toomey, global head insurance fraud product manager at BAE Systems. But he argues that the industry is not matching this innovation in its counter-fraud approach. “As far as I am aware, there are no insurers scanning the dark web for insight into how they are being targeted, but it can be done,” he says.

This need to monitor for criminal activity is not, however, limited to external threats.

Fighting fraud from within

While significant investment is focused externally, vulnerability inside companies is just as potent. Financial criminals often hide – very well – in plain sight. These perpetrators come

¹⁰ <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-underground-job-market/>



“Criminals are so sophisticated that they have catalogues outlining which companies will pay what in a claim” Dennis Toomey

in through the front door.

Toomey says this is a woefully under-rated issue. “Insurers are building huge cyber defences, but they are missing the insider threat of people who have been hired by the company but are working for fraudsters.”

Such people collate information for the benefit of criminals.

“Criminals are so sophisticated that they have catalogues outlining which companies will pay what in a claim and even which individual claims handlers are likely to pay the most. Criminals have infiltrated the whole production line.”

Insiders are, in fact, the most common facilitators of fraud, with junior employees perpetrating 39 per cent of it, ex-employees committing 34 per cent and senior or middle management 27 per cent, according to Kroll¹¹.

For example, Eric Garcia-Cebollero¹² was employed as a large loss specialist by Florida-based Citizens Property Insurance with authority to approve claims of up to \$50,000 in value. He used this power to demand bribes from contractors for business referrals and to push through fraudulent claims on behalf of policyholders.

In 2015 he was caught and arrested by the police – who proceeded to recruit him as an undercover police operative to ensnare his accomplices.

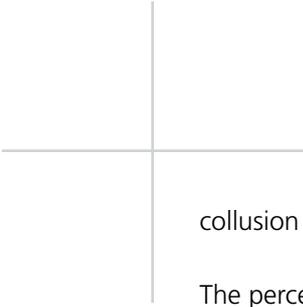
Garcia-Cebollero continued to work at Citizens Property Insurance for a further two years with the company unaware of either the fraud or his new dual role. They remained so until early 2018 when the Miami Herald informed them of the situation.

This unusual but not isolated case highlights the difficulty in identifying internal fraud. But advances in technology, with forward-thinking companies judiciously employing data analysis to identify suspicious behaviour among employees, offers new power to insurers.

Such has been the success of analytics that moves are being made to apply the approach elsewhere. Companies are starting to apply these tools to HR data to identify internal

¹¹ http://www.fraudexaminer.in/docs/Kroll_Global_Fraud_Risk_Report_2017_18.pdf

¹² <https://www.miamiherald.com/news/local/crime/article207492209.html>



collusion with fraudulent third parties.

The percentage of companies employing user-behaviour analytics tools has risen significantly, from 42 per cent in 2017 to 94 per cent in 2018, according to software firm CA Technologies¹³.

However, analysis in isolation can only ever be partially effective. The structural and cultural silos that exist in many large insurance companies could, unwittingly, be part of the wider problem.

“You often find that internal audit groups, compliance groups and external fraud groups do not collaborate,” says Toomey.

“There is no overall intelligence level platform to look at employee sentiment or what is happening in the wider business which gives the ethically challenged the opportunity to exploit a carrier’s siloed defence systems.”

It's all about the data

The size and complexity of many insurance companies makes it difficult to get a real-time snapshot of what is happening both internally and externally. Many are turning to Big Data and Artificial Intelligence (AI) to provide an overview.

Anti-fraud use has thus far been limited to identifying individual incidences of criminality. Here, too, silos limit effectiveness, with Artificial Intelligence deployment often isolated within one department.

But early signs are encouraging and awareness of AI’s potential in combating fraud is growing. Forty-nine per cent of finance senior executives expected their firms to use AI for risk assessment within the next three years, a recent Baker McKenzie¹⁴ survey found.

¹³ <https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf>

¹⁴ http://f.datasrvr.com/fr1/516/80536/Baker_McKenzie_Ghosts_in_the_Machine_2016.pdf#page=2&zoom=auto,-112,617



The percentage of companies employing **user-behaviour analytics** tools has risen significantly, from 42 per cent in 2017 to 94 per cent in 2018



Technology is crucial in the fight against crime. As Cate Wright, global insurance product manager at BAE Systems, points out, fraudsters don't discriminate – they will attack any line of insurance that offers the opportunity to make money. Like criminals, insurers must ensure they can monitor activity right across their portfolios.

Wright believes a culture of collaboration and data sharing is finally growing in the UK. To exploit this development to its full effect, she says, insurers need to move from a largely reactive anti-fraud attitude to a forward-thinking, predictive and future-proof one.

Analytics: don't just react, predict

Predictive analytics, based on machine learning, moves away from generic scoring to identify risk. "It allows us to learn outcomes and then feed them back in so we can really start predicting the likelihood of risk and the potential outcome," says Wright.

This technological foresight, she believes, can not only assist in identifying fraud, but can also improve customer experience by allowing insurers to usher genuine customers through the validation process much faster.

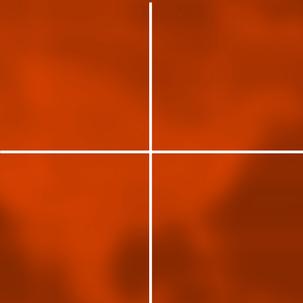
Examples of the kinds of problems which predictive analytics might prevent abound, with the healthcare sector particularly at risk from insider data breach due to the sensitivity of its information. In 2017, an employee of Bupa Global¹⁵ was able to remove and make available to other parties the personal details of 547,000 customers.

Financial crime is everybody's problem

Data analytics, like other technological solutions, must be fully integrated and used broadly across an organisation to maximise its potential. Yet IT security or anti-fraud professionals often feel that they are seen as solely responsible for protecting their business from crime.

This is a company-wide issue and one for which – in future – the responsibility to meet threats must be shared. Ensuring that communication on matters that can be complex

¹⁵ <https://www.telegraph.co.uk/technology/2018/09/28/bupa-fined-175000-employee-stole-500000-customer-records-tried/>



Create an account

 Username or email

 Password

Login

Remember me [Need help?](#)

and technical is accessible, encouraged and valued is key. The danger is that while these remain largely incomprehensible to the non-expert, so too do the problems they tackle.

Simon Viney, cyber security financial services lead at BAE Systems says: “Even when the board does have the awareness of these risks, they don’t necessarily have the understanding to effectively challenge what they are being told by experts.”

Bringing technical expertise to the boardroom

Viney insists that forward-thinking insurers must start recruiting at board and non-exec level specifically to plug these knowledge gaps in order to combat cyber-enabled fraud. By fostering expertise at senior levels and encouraging the technically knowledgeable to communicate effectively, businesses can start evaluating and tackling the threats in a more constructive way. Almost three-quarters (71 per cent) of board members involved in 2017 BAE Systems¹⁶ research considered cyber security the most significant challenge facing their business.

Progress is being made on this front. Nearly a quarter (22 per cent) of executives intend to expand their current use of board engagement to mitigate cyber risk, according to Kroll¹⁷. A further 40 per cent were planning new initiatives to focus board members on insider cyber crime in the next 12 months.

And there is an equally encouraging picture in the C-suite when it comes to fraud awareness. In its 2016 Global Forensics Data Analytics Survey¹⁸, EY found that 74 per cent of C-suite respondents agreed they had to do more to improve anti-fraud

¹⁶ <https://www.baesystems.com/en/cybersecurity/feature/cyber-defence-monitor-2017--intelligence-disconnect>

¹⁷ http://www.fraudexaminer.in/docs/Kroll_Global_Fraud_Risk_Report_2017_18.pdf

¹⁸ [https://www.ey.com/Publication/vwLUAssets/EY-shifting-into-high-gear-mitigating-risks-and-demonstrating-returns-63x82/\\$-](https://www.ey.com/Publication/vwLUAssets/EY-shifting-into-high-gear-mitigating-risks-and-demonstrating-returns-63x82/$-)

procedures and 63 per cent said they would commit at least half of their data analytics spending to proactively identifying fraud.

But for Toomey, the approaches to fraud and cyber defences are still too fractured and divergent. He believes that only when insurers grasp the unified nature of the threat will real progress be made.

A reluctance to report cyber crime is currently allowing criminals to operate in the shadows created by the insurance industry

“The answer is to break down the internal silos between cyber and fraud by establishing a central intelligence platform in addition to bringing this experience to the board room.

“This will help organisations be more analytical and proactive in defending their assets, people and customers. Education, awareness and internal collaboration will go a long way to tackling this problem.”

In the adjacent industry of banking, several institutions have begun to tackle this issue¹⁹, removing the data-sharing barriers that surround cyber, fraud and compliance teams and encouraging more collaborative methods of working.

Companies that can bridge this operational and cultural divide will be best placed to head off criminal attacks in future.

Fraud and cyber are one and the same

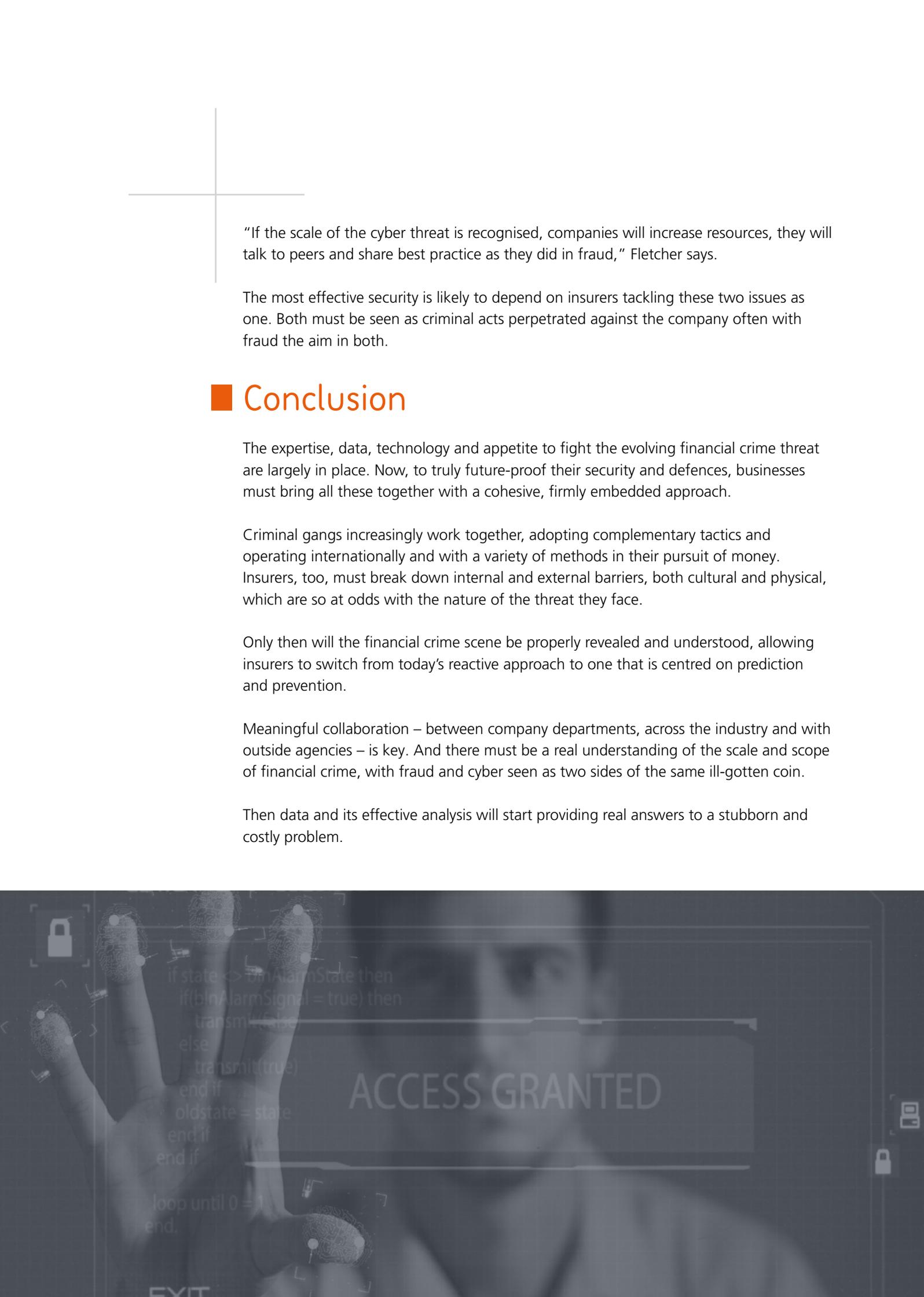
In breaking down barriers to communication, comprehension and collaboration, insurers should identify previously unseen common ground between fraud and cyber risks. The result – an ability to target similar defences at both threats – will help build security that is both more robust and more cost-effective.

Ben Fletcher, director of the Insurance Fraud Bureau (IFB), believes that while cyber weapons may be a new problem, the methods and solutions need not always be so. “The [criminal] tactics are not terribly dissimilar – making patterns look like isolated incidents, for example.”

A reluctance to report cyber crime is currently allowing criminals to operate in the shadows created by the insurance industry, but Fletcher predicts that this will change, mirroring the fraud-space pattern.

FILE/EY-shifting-into-high-gear-mitigating-risks-and-demonstrating-returns.pdf

¹⁹ <https://www.baesystems.com/en/cybersecurity/feature/collaborative-steps-in-the-fight-against-financial-crime>



“If the scale of the cyber threat is recognised, companies will increase resources, they will talk to peers and share best practice as they did in fraud,” Fletcher says.

The most effective security is likely to depend on insurers tackling these two issues as one. Both must be seen as criminal acts perpetrated against the company often with fraud the aim in both.

■ Conclusion

The expertise, data, technology and appetite to fight the evolving financial crime threat are largely in place. Now, to truly future-proof their security and defences, businesses must bring all these together with a cohesive, firmly embedded approach.

Criminal gangs increasingly work together, adopting complementary tactics and operating internationally and with a variety of methods in their pursuit of money. Insurers, too, must break down internal and external barriers, both cultural and physical, which are so at odds with the nature of the threat they face.

Only then will the financial crime scene be properly revealed and understood, allowing insurers to switch from today’s reactive approach to one that is centred on prediction and prevention.

Meaningful collaboration – between company departments, across the industry and with outside agencies – is key. And there must be a real understanding of the scale and scope of financial crime, with fraud and cyber seen as two sides of the same ill-gotten coin.

Then data and its effective analysis will start providing real answers to a stubborn and costly problem.

What next?

Insurers who prepare for the future early are better protected – but this is not solely related to buying the latest solution. Organisational development has at least as significant a role.

Countering international networks

Insurers need to be aware of fraud typologies and criminal tactics hopping across international borders and lines of business: today's cash-for-crash motor fraud is often tomorrow's holiday insurance scam. Holistic views of customers and entities help but it takes industry bodies, regulators and law enforcement collaborating with engaged insurers.

Build technical expertise in the board room

Understanding how technology counters and assists crimes is vital. This calls for skill sets at board level that weren't necessary 10 years ago. It's also the responsibility of leaders on counter-fraud, cyber security and SIU to educate their board.

Coupling fraud and cyber

Cyber security is a key consideration at all levels of future-proofed insurers. Collaborative working to understand the blended threat is vital – and that goes for suppliers and insurers.

For more information go to: www.baesystems.com/insuranceinsights

Contact us

E: learn@baesystems.com

W: baesystems.com/insuranceinsights

Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155

UK: 0808 168 6647

Australia: 1800 825 411

International: +44 1483 817491

E: cyberresponse@baesystems.com

Copyright © BAE Systems plc 2019. All rights reserved. BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc. BAE Systems Applied Intelligence Limited registered in England & Wales (No.1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7RQ. No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems Applied Intelligence.



[linkedin.com/company/baesystemsai](https://www.linkedin.com/company/baesystemsai)



twitter.com/baesystems_ai

BAE SYSTEMS