Monday, October 5, 2020

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next

Dear members and friends,

This is an interesting title for a presentation: *"Technology exposes banks' vulnerabilities"*.

Pentti Hakkarainen, member of the Supervisory Board of the European Central Bank, gave this presentation at the *Institute of International Finance Digital Interchange: The Global Dialogue on Digital Finance* (Frankfurt am Main).

He said: "Reaping the benefits of information technology (IT) is not a new challenge for the banking industry. As a bank CEO in the 90s, I saw giant leaps made in technology. Owing to the severe economic crisis at the time, Nordic banks had no choice but to innovate and make use of technology to become more efficient.

It is therefore no surprise to me that European banks were technologically ready to handle the coronavirus (COVID-19) crisis. They have continued to deliver banking services smoothly throughout this challenging period, showing that their IT systems were up to the job of keeping the show on the road.

However, operational resilience alone will not be enough for banks to survive and thrive in the coming decades. We are seeing profound long-term technological changes that will alter the way customers demand and receive financial products. Some of the expected unbundling of traditional services is already occurring, and the potential exists for powerful new competitors to enter the market.

In the light of these circumstances, banks must pursue ambitious digital transformation plans. Customers' demands for convenience require banks

to have global state-of-the-art technological service models. Merely adopting advanced technologies to improve internal processes is not enough. Satisfying the needs of sophisticated customers in today's increasingly competitive environment will require innovation to place the focus on the customer service experience."

He continued: "COVID-19 has put operational resilience to the test. The COVID-19 crisis has challenged the digital capabilities of banks under European supervision, both in terms of their interactions with customers and their internal operations.

At the height of the lockdown in late March, around 60% of the staff of large European banks were working remotely and more than 20% of branches were closed. For the time being, banks envisage only a gradual return to the office - on average, 40% of bank employees are currently still working from home and around 5% of branches remain closed.

So far, banks' IT infrastructures have stood up well to this test. In particular, almost all banks have managed to continue providing services to their customers during these extraordinary times. Similarly, in the face of heightened cyber risks during this period, banks have not suffered any major setbacks to their operational resilience.

This shows that they have done their job in adopting the technology needed to run their businesses digitally."

He continued: "Digitalisation has spurred new market practices that encourage traditional banking businesses to be split into their constituent parts, such as the provision of payment services, lending and deposit-taking.

These services are offered by new market players, including both digital banks that focus on providing a platform, and non-bank entrants. This unbundling of banking and other financial services enables new players to enter consolidated markets while putting pressure on incumbents.

Fintech firms enter financial markets by offering payment, peer-to-peer lending or crowdfunding services to underserved clients and younger, more tech-savvy customers. By unbundling traditional financial services and focusing on single activities in the value chain, fintechs introduce new business models and build on their distinct comparative advantages.

They may establish and promote themselves as pure online service providers, harvest new sources of data, and employ artificial intelligence, including machine learning and other methods, to offer financial products

tailored to client preferences. Unlike incumbent banks, fintech-oriented banks and other fintech companies are not usually burdened by legacy IT systems.

Fintech firms may also re-bundle financial activities. They use user-friendly online or mobile phone applications in conjunction with other innovative channels to provide financial investment services, access to crowdfunding platforms, or instant comparisons of financial services."

Interesting presentation. It is true, technology exposes banks' vulnerabilities. I remember what Linus Torvalds (the principal developer of the Linux kernel) has said: Microsoft is not evil, they just make really crappy operating systems. I disagree with Linus, but I understand the point.

You can read the presentation at:
https://www.bankingsupervision.europa.eu/press/speeches/date/2020/html/ssm.sp200916~e52c53cd6b.en.html

Welcome to our Top 10 list.

Best regards,

George Lekatis
President of the IARCP
1200 G Street NW Suite 800,
Washington DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA
Tel: (302) 342-8828

Number 1 (Page 7)

Outlook for the global financial system in the wake of the pandemic

Hyun Song Shin, Economic Adviser and Head of Research at the BIS, published in Nikkei

Number 2 (Page 11)

Worldwide Threats to the Homeland

Christopher Wray, Director, Federal Bureau of Investigation, Statement Before the House Homeland Security Committee, Washington, D.C.

Number 3 (Page 22)

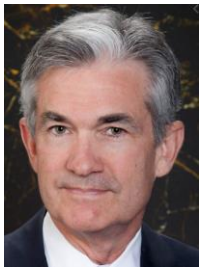
About the Standard-Setting Process

PCAOB
Public Company Accounting Oversight Board

Number 4 (Page 25)

Coronavirus Aid, Relief and Economic Security Act

Jerome H Powell, Chair of the Board of Governors of the Federal Reserve System, before the Committee on Financial Services, US House of Representatives, Washington DC.



Number 5 (Page 29)

Promoting the soundness and efficiency of our insurance sector - recommencing the IPSA and Solvency Standard review

Geoff Bascand, Deputy Governor and General Manager of Financial Stability of the Reserve Bank of New Zealand, to the Insurance Council of New Zealand, Wellington.

RESERVE BANK OF NEW ZEALAND
TE PŪTEA MATUA

Number 6 (Page 33)

Tip & Referral Center
Enforcement Tips, Referrals, Complaints, and Other Information

PCAOB
Public Company Accounting Oversight Board

Number 7 (Page 35)

BIS Statistics: Charts

BIS Quarterly Review, September 2020, International banking and financial market developments

BIS

Number 8 (Page 37)

UEFI Secure Boot Customization

National Security Agency, Cybersecurity Technical Report

Number 9 (Page 40)

New cyberattacks targeting U.S. elections

Tom Burt - Corporate Vice President, Customer Security & Trust

Microsoft

Number 10 (Page 46)

Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally

Two Defendants Arrested in Malaysia; Remaining Five Defendants, One of Whom Allegedly Boasted of Connections to the Chinese Ministry of State Security, are Fugitives in China

Number 1

Outlook for the global financial system in the wake of the pandemic

Hyun Song Shin, Economic Adviser and Head of Research at the BIS, published in Nikkei

The Covid-19 crisis is three shocks rolled into one. Above all, it is a health crisis that has brought untold human suffering.

Second, by disrupting everyday life so severely, it brought an economic sudden stop, especially in those countries that imposed widespread lockdowns to contain the virus.

However, even countries with no lockdowns have suffered sharp declines in economic activity, suggesting that the virus must be contained to sustain economic activity. And third, the pandemic unleashed a financial sudden stop when significant segments of the global financial system experienced acute stress.

The financial sudden stop bears some resemblance to the stresses seen during the Great Financial Crisis, but there are important differences. The crisis of 2007-09 was essentially a global banking crisis, with overextended banks at its epicentre. The real economy became the collateral damage as these banks stumbled and fought for survival.

This time round, the direction of the shock has been reversed. Banks have been at the receiving end of the financial stress and economic sudden stop that resulted from the exogenous shock of Covid-19.

The banking sector has proved resilient so far. Post-crisis regulation has had a hand in strengthening the capital and liquidity positions of banks. Plus, they are now a smaller part of the financial system than they were before the Great Financial Crisis, following a long period of slower lending growth.

For all these reasons, banks were not in the eye of the storm. Instead, the strains were felt most by market-based financial intermediaries and in bond and money markets.

As the stresses reverberated within the system, key short-term funding markets came under severe stress, including the crucially important dollar funding markets that underpin the global financial system.

Although banks were not the origin of the crisis, they cannot expect to remain unscathed.

As the economic downturn starts to bite, the immediate liquidity phase of the crisis is giving way to the solvency phase, and banks will undoubtedly bear the brunt of the wave of bad loans and insolvencies affecting weaker businesses, especially in those sectors the pandemic has hit the hardest.

A sign of banks' apprehension is the soaring provisioning levels for loan losses. At the same time, surveys show a significant tightening of lending standards.

The triple shock and its likely impact on the banking sector largely explain why fiscal policy has taken centre stage in the economic policy response to the pandemic.

Fiscal authorities globally moved swiftly to implement very large direct budgetary packages amounting to 6% of GDP, augmented with another 10% of GDP in loans and guarantees.

At the outset, actions by many authorities across the world to enable direct transfers to households helped to alleviate immediate hardship resulting from the lockdowns.

Meanwhile grants and loans to businesses allowed them to meet essential outlays. Such prompt actions prevented the wholesale unravelling of the intricate web of economic relationships between firms and their workers, suppliers and customers, all of which are crucial for maintaining the fabric of a modern economy.

Credit guarantees and funding for lending schemes have been instrumental in mitigating the tightening of credit availability to businesses.

Some tightening of credit standards will be unavoidable as the economic downturn and restructuring of businesses run their course, but the objective is to lean against a sharp and abrupt tightening to keep credit flowing to support the recovery when the worst of the virus passes.

One of the challenges now facing authorities is to ensure that unviable businesses can be restructured in an orderly way rather than indiscriminately under financial stress.

In step with the fiscal response, central banks have intervened in financial markets on a massive scale, through both collateralised lending and direct asset purchases.

These liquidity injections and asset purchases have restored the orderly functioning of financial markets and alleviated stresses in short-term funding markets.

Particularly important were the Federal Reserve's central bank dollar swap facilities, which it extended to a larger number of counterparty central banks.

The Fed also expanded its dollar liquidity toolkit to allow lending against treasury collateral. These actions quelled the funding stresses in the critically important dollar funding market.

Partly as a result, emerging market economy (EME) central banks were able to depart from their usual playbook for financial crisis monetary policy, which calls for raising interest rates sharply in the face of currency depreciation and portfolio outflows. Instead, they eased monetary policy and managed to cut interest rates.

Indeed, many EME central banks rolled out bond purchase programmes for domestic currency sovereign bonds. The bond purchases were small and were aimed at restoring market functioning rather than engaging in quantitative easing.

Loosening monetary policy in the face of a financial crisis was highly unusual, and signalled a coming of age of EME central banks, reaping the greater monetary policy credibility built up over recent years.

However, the more benign environment of a weaker dollar and the more accommodative global liquidity conditions engineered by the major central banks have been key enabling elements.

Revealingly, whereas EMEs were able to loosen monetary policy aggressively, their fiscal policy response was more modest.

Compared with advanced economy packages that amounted to around 22% of GDP, fiscal packages in EMEs were much smaller, at around 6% of GDP, even though EMEs arguably need a still larger fiscal response to the pandemic.
One reason for their greater caution may be the assessment that they have less fiscal space, given domestic investors' limited capacity to absorb government debt sales, and foreign investors' limited appetite to do so.

The alternative would be monetary financing by the central bank, but on this score memories are still fresh from the financial crises of the 1980s, when monetary financing in some EMEs led to collapsing currencies, monetary instability and sharply higher inflation.

EMEs have so far largely avoided the pitfalls of monetary financing. Financial conditions have remained accommodative on the back of a weaker dollar, which tends to coincide with greater risk-taking capacity of market participants through the financial channel of exchange rates.

However, it would be foolhardy to be swayed too much by prevailing market conditions and expect the trend to continue indefinitely. Indeed, the longer the dollar's weakness persists, the larger will be the risk-taking exposures that will come under stress when the dollar cycle eventually turns.

Ultimately, the prospects for the global economy will depend on the pandemic's trajectory. If the virus lingers in large parts of the world, or if there is a resurgence, more of the fiscal and monetary interventions seen so far will be needed.

The challenge facing authorities is that fiscal space varies widely across countries. For EMEs with a history of monetary instability, it is more limited.

Even advanced economies whose currencies enjoy reserve currency status face theoretical limits to their fiscal firepower, even if prevailing market conditions obscure the exact boundaries of available fiscal space.

As central banks come under pressure to accommodate additional fiscal expenditure through asset purchases, the risk of fiscal dominance will pose new challenges to central banks' policy frameworks. To chart the course ahead, joined-up thinking from a global perspective and an emphasis on long-term monetary stability will be more important than ever.

Number 2

Worldwide Threats to the Homeland

Christopher Wray, Director, Federal Bureau of Investigation, Statement Before the House Homeland Security Committee, Washington, D.C.

Good afternoon, Chairman Thompson, Ranking Member Rogers, and members of the committee. Thank you for the opportunity to appear before you today to discuss the current threats to the United States homeland. I am pleased to be here representing the nearly 37,000 dedicated men and women of the FBI.

While the COVID-19 pandemic has presented unique and unprecedented challenges to the FBI workforce, I am proud of their dedication to our mission of protecting the American people and upholding the Constitution. Hostile foreign actors, violent extremists, and opportunistic criminal elements have seized upon this environment. As a result, we are facing aggressive and sophisticated threats on many fronts.

Whether it is terrorism now moving at the speed of social media, or the increasingly blended threat of cyber intrusions and state-sponsored economic espionage, or malign foreign influence and interference or active shooters and other violent criminals threatening our communities, or the scourge of opioid trafficking and abuse, or hate crimes, human trafficking, crimes against children—the list of threats we are worried about is not getting any shorter, and none of the threats on that list are getting any easier.

Counterterrorism

Preventing terrorist attacks remains the FBI's top priority. However, the threat posed by terrorism—both international terrorism (IT) and domestic violent extremism—has evolved significantly since 9/11.

The greatest threat we face in the homeland is that posed by lone actors radicalized online who look to attack soft targets with easily accessible weapons. We see this lone actor threat manifested both within domestic violent extremists (DVEs) and homegrown violent extremists (HVEs), two distinct sets of individuals that generally self-radicalize and mobilize to violence on their own.

DVEs are individuals who commit violent criminal acts in furtherance of ideological goals stemming from domestic influences, such as racial bias and anti-government sentiment. HVEs are individuals who have been radicalized primarily in the United States, and who are inspired by, but not receiving individualized direction from, foreign terrorist organizations (FTOs).

Many of these violent extremists, both domestic and international, are motivated and inspired by a mix of ideological, sociopolitical, and personal grievances against their targets, which recently have more and more included large public gatherings, houses of worship, and retail locations.

Lone actors, who by definition are not likely to conspire with others regarding their plans, are increasingly choosing these soft, familiar targets for their attacks, limiting law enforcement opportunities for detection and disruption ahead of their action.

DVEs pose a steady and evolving threat of violence and economic harm to the United States. Trends may shift, but the underlying drivers for domestic violent extremism—such as perceptions of government or law enforcement overreach, sociopolitical conditions, racism, anti-Semitism, Islamophobia, misogyny, and reactions to legislative actions—remain constant.

As stated above, the FBI is most concerned about lone offender attacks, primarily shootings, as they have served as the dominant lethal mode for domestic violent extremist attacks. More deaths were caused by DVEs than international terrorists in recent years. In fact, 2019 was the deadliest year for domestic extremist violence since the Oklahoma City bombing in 1995.

The top threat we face from domestic violent extremists stems from those we identify as racially/ethnically motivated violent extremists (RMVE). RMVEs were the primary source of ideologically motivated lethal incidents and violence in 2018 and 2019 and have been considered the most lethal of all domestic extremists since 2001. Of note, the last three DVE attacks, however, were perpetrated by anti-government violent extremists.

The spate of attacks we saw in 2019 underscore the continued threat posed by DVEs and perpetrators of hate crimes. The FBI works proactively to prevent acts of domestic terrorism and hate crimes. For example, in November 2019, the Denver Joint Terrorism Task Force arrested Richard Holzer on federal charges of attempting to obstruct religious exercise by force using explosives.

This disruption is just one example of the strength of our Domestic Terrorism-Hate Crimes (DT-HC) Fusion Cell. Our Counterterrorism

Division (CTD) and Criminal Division (CID), working together, were able to prevent a potential terrorist attack before it occurred and, for the first time in recent history, make a proactive arrest on a hate crimes charge.

Through the DT-HC Fusion Cell, subject-matter experts from both CTD and CID work in tandem to innovatively use investigative tools and bring multiple perspectives to bear in combating the intersecting threats of domestic terrorism and hate crimes, preventing attacks and providing justice to victims.

We recognize that the FBI must be aware not just of the domestic violent extremism threat, but also of threats emanating from those responding violently to First Amendment-protected activities. In the past, we have seen some violent extremists respond to peaceful movements through violence rather than non-violent actions and ideas.

The FBI is involved only when responses cross from ideas and constitutionally protected protests to violence. Regardless of the specific ideology involved, the FBI requires that all domestic terrorism investigations be predicated based on activity intended to further a political or social goal, wholly or in part involving force, coercion, or violence, in violation of federal law.

HVEs and FTOs have posed a persistent threat to the nation and to U.S. interests abroad, while their tradecraft, tactics, and target sets have evolved. The international terrorism threat to the U.S. has expanded from sophisticated, externally directed FTO plots to include individual attacks carried out by HVEs who are inspired by designated terrorist organizations. As stated above, the FBI assesses HVEs are the greatest, most immediate international terrorism threat to the homeland.

These individuals are FTO-inspired individuals who are in the U.S., have been radicalized primarily in the U.S., and are not receiving individualized direction from FTOs. We, along with our law enforcement partners, face significant challenges in identifying and disrupting HVEs. This is due, in part, to their lack of a direct connection with an FTO, an ability to rapidly mobilize without law enforcement detection, and their frequent use of encrypted communications.

Many FTOs use various digital communication platforms to reach individuals they believe may be susceptible and sympathetic to violent terrorist messages. However, no group has been as successful at drawing people into its perverse ideology as ISIS, which has proven dangerously competent at employing such tools. ISIS uses traditional media platforms as well as widespread social media campaigns to propagate its ideology.

Terrorists in ungoverned spaces—both physical and virtual—readily disseminate propaganda and training materials to attract easily influenced individuals around the world to their cause.

With the broad distribution of social media, terrorists can spot, assess, recruit, and radicalize vulnerable persons of all ages in the U.S. either to travel to foreign lands or to conduct an attack on the homeland. Through the internet, terrorists anywhere overseas now have direct access to our local communities to target and recruit our citizens and spread their message faster than was imagined just a few years ago.

We remain concerned that groups such as the Islamic State of Iraq and ash-Sham (ISIS) and al Qaeda intend to carry out large-scale attacks in the U.S. Despite their territorial defeat in Iraq and Syria, ISIS remains relentless and ruthless in its campaign of violence against the West and has aggressively promoted its hateful message, attracting like-minded violent extremists.

The message is not tailored solely to those who overtly express signs of radicalization. It is seen by many who use messaging apps and participate in social networks. Ultimately, many of the individuals drawn to ISIS seek a sense of belonging.

Echoing other terrorist groups, ISIS has advocated lone offender attacks in Western countries. Recent ISIS videos and propaganda have specifically advocated attacks against soldiers, law enforcement, and intelligence community personnel.

As noted above, ISIS is not the only terrorist group of concern. Al Qaeda maintains its desire for large-scale, spectacular attacks. While continued counterterrorism pressure has degraded the group's Afghanistan-Pakistan senior leadership, in the near term, al Qaeda is more likely to focus on building its international affiliates and supporting small-scale, readily achievable attacks in key regions such as East and West Africa.

Simultaneously, over the last year, propaganda from al Qaeda leaders seeks to inspire individuals to conduct their own attacks in the U.S. and the West. For example, the December 2019 attack at Naval Air Station Pensacola demonstrates that groups such as al Qaeda continue to be interested in encouraging attacks on U.S. soil.

The FBI regularly reviews intelligence to ensure that we are appropriately mitigating threats from any place by any actor, and the possible violent responses and actions. We are sensitive to First Amendment-protected activities during investigative and intelligence efforts so as to ensure that

our investigative actions remain aligned with our authorities and are conducted with the appropriate protections in place for privacy and civil liberties.

As the threat to the United States and U.S. interests evolves, we must adapt and confront these challenges, relying heavily on the strength of our federal, state, local, tribal, and international partnerships.

The FBI uses all lawful investigative techniques and methods to combat these terrorist threats to the United States. Along with our domestic and foreign partners, we are collecting and analyzing intelligence concerning the ongoing threat posed by violent extremists motivated by any ideology and desire to harm Americans and U.S. interests.

We continue to encourage information sharing, which is evidenced through our partnerships with many federal, state, local, and tribal agencies assigned to Joint Terrorism Task Forces around the country. Be assured, the FBI continues to strive to work and share information more efficiently, and to pursue a variety of lawful methods to help stay ahead of these threats.

Election Security

In less than two months, Americans will exercise one of their most important and cherished freedoms: the right to vote in a democratic election. Our nation is confronting multi-faceted foreign threats seeking to both influence our national policies and public opinion and cause harm to our national dialogue.

The FBI and our interagency partners remain concerned about, and focused on, the covert and overt influence measures used by certain adversaries in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic processes.

Foreign influence operations—which include covert, coercive, or corrupt actions by foreign governments to influence U.S. political sentiment or public discourse or interfere in our processes themselves—are not a new problem. But the interconnectedness of the modern world, combined with the anonymity of the internet, have changed the nature of the threat and how the FBI and its partners must address it.

This year's election cycle, amid the COVID-19 pandemic, provides ample opportunity for hostile foreign actors to conduct disinformation campaigns and foreign influence operations in an effort to mislead, sow discord, and,

ultimately, undermine confidence in our democratic institutions and values and in our government's response to our current health crisis.

Foreign influence operations have taken many forms and used many tactics over the years. Most widely reported these days are attempts by adversaries—hoping to reach a wide swath of Americans covertly from outside the United States—to use false personas and fabricated stories on social media platforms to discredit U.S. individuals and institutions.

The FBI is the lead federal agency responsible for investigating foreign influence operations. In the fall of 2017, the Foreign Influence Task Force (FITF) was established to identify and counteract malign foreign influence operations targeting the United States.

The FITF is led by the Counterintelligence Division and is composed of agents, analysts, and professional staff from the Counterintelligence, Cyber, Counterterrorism, and Criminal Investigative Divisions.

It is specifically charged with identifying and combating foreign influence operations targeting democratic institutions and values inside the United States. In all instances, the FITF strives to protect democratic institutions and public confidence, develop a common operating picture, raise adversaries' costs, and reduce their overall asymmetric advantage.

The task force brings the FBI's national security and traditional criminal investigative expertise under one umbrella to prevent foreign influence in our elections. This better enables us to frame the threat, to identify connections across programs, to aggressively investigate as appropriate, and—importantly—to be more agile.

Coordinating closely with our partners and leveraging relationships we have developed in the technology sector, we had a number of instances where we were able to quickly relay threat indicators that those companies used to take swift action, blocking budding abuse of their platforms.

Following the 2018 midterm elections, we reviewed the threat and the effectiveness of our coordination and outreach. As a result of this review, we further expanded the scope of the FITF. Previously, our efforts to combat malign foreign influence focused solely on the threat posed by Russia.

Utilizing lessons learned over the last year and half, the FITF is widening its aperture to confront malign foreign operations of China, Iran, and other global adversaries. To address this expanding focus and wider set of adversaries and influence efforts, we have also added resources to maintain permanent "surge" capability on election and foreign influence threats.

We have also further refined our approach. All efforts are based on a three-pronged approach, which includes investigations and operations, information and intelligence sharing, and a strong partnership with the private sector. Through the efforts of the FITF and lessons learned from both the 2016 and 2018 elections, the FBI is actively engaged in identifying, detecting, and disrupting threats to our elections and ensuring both the integrity of our democracy is preserved and the will of the American people is fulfilled.

Protecting policymakers is an important part of our efforts to combat malign foreign influence and protect our elections. As you are aware, the FBI and our interagency partners have been providing ongoing election security threat briefings to Congress. We will continue to do so throughout the fall and into the future, where there is actionable intelligence.

Lawful Access

I want to turn now to an issue continuing to limit law enforcement's ability to disrupt these increasingly insular actors. We are all familiar with the inability of law enforcement agencies to access data, even with a lawful warrant or court order, due to "end-to-end" encryption.

Increasingly, device manufacturers and communications service providers have employed encryption in such a manner that only the users or parties to the communications can access the content of the communications or devices. This is known as end-to-end encryption.

This development has meant that, in recent years, the FBI has observed a decline in its ability to gain access to the content of both domestic and international terrorist communications due to the widespread adoption of encryption for internet traffic and the prevalence of mobile messaging apps using end-to-end encryption as default.

The FBI certainly recognizes how encryption increases the overall safety and security of the internet for users. But in fulfilling the FBI's duty to the American people to prevent acts of terrorism, this kind of end-to-end encryption creates serious challenges.

Accessing content of communications by, or data held by, known or suspected terrorists pursuant to judicially authorized, warranted legal process is getting more and more difficult.

The online, encrypted nature of radicalization, along with the insular nature of most of today's attack plotters, leaves investigators with fewer dots to connect. As was evident in the December 9, 2019, shooting at Naval Air Station Pensacola that killed three U.S. sailors and severely wounded eight

other Americans, deceased terrorist Mohammed Saeed Alshamrani was able to communicate using warrant-proof, end-to-end encrypted apps deliberately to evade detection by law enforcement. It took the FBI several months to access information in his phones, during which time we did not know whether he was a lone wolf actor or whether his associates may have been plotting additional terrorist attacks.

If law enforcement loses the ability to detect criminal activity because communication between subjects—data in motion—or data held by subjects— data at rest—is encrypted in such a way making content inaccessible, even with a lawful order, our ability to protect the American people will be degraded.

Providers and law enforcement must continue to collaborate to explore possible technical solutions that would provide security and privacy to those using the internet while also contributing to the FBI's ability to complete its mission.

Despite the successes that result from the hard work of the men and women of the FBI, our Joint Terrorism Task Forces, and our partners across the government, terrorism continues to pose a persistent threat to the homeland and our interests overseas.

China Threat

The greatest long-term threat to our nation's information and intellectual property and to our economic vitality is the counterintelligence and economic espionage threat from China. It is a threat to our economic security and by extension, to our national security.

As you have seen from the recent closure of the Chinese Consulate in Houston, this issue is not just an intelligence issue, or a government problem, or a nuisance largely just for big corporations who can take care of themselves.

Our adversaries' targets are our nation's core economic assets—our information and ideas, our innovation, our research and development, our technology. No country poses a broader, more severe threat to those assets than China. It is the people of the United States who are the victims of what amounts to Chinese theft on a scale so massive that it represents one of the largest transfers of wealth in human history. If you are an American adult, it is more likely than not that China has stolen your personal data.

In 2017, the Chinese military conspired to hack Equifax and made off with the sensitive personal information of 150 million Americans—we are talking

nearly half of the American population and most American adults. Our data is not the only thing at stake here—so is our health, livelihood, and security.

The FBI is opening a new China-related counterintelligence case approximately every 10 hours. Of the nearly 5,000 active FBI counterintelligence cases currently underway across the country, almost half are related to China. And at this very moment, China is working to compromise American health care organizations, pharmaceutical companies, and academic institutions conducting essential COVID-19 research. They are going after cost and pricing information, internal strategy documents, personally identifiable information—anything that can give them a competitive advantage.

It is important to be clear: This is not about the Chinese people as a whole, and certainly not about Chinese Americans as a group, but it is about the Chinese government and the Chinese Communist Party. Every year, the United States welcomes more than 100,000 Chinese students and researchers into this country.

For generations, people have journeyed from China to the United States to secure the blessings of liberty for themselves and their families—and our society is better for their contributions. So, when the FBI's refers to the threat from China, we mean the government of China and the Chinese Communist Party.

Confronting this threat effectively does not mean that we should not do business with the Chinese. It does not mean that we should not host Chinese visitors. It does not mean that we should not welcome Chinese students or coexist with China on the world stage. But it does mean that when China violates our criminal laws and international norms, we are not going to tolerate it, much less enable it.

The FBI and our partners throughout the U.S. government will hold China accountable and protect our nation's innovation, ideas, and way of life—with the help and vigilance of the American people.

Cyber

With the advent of the COVID-19 pandemic, the nature of the cyber threat has become increasingly concerning. As more individuals telework and increasingly use the cloud, we encounter less secure networks. As a result, the scope of our cyber threats has changed, the impact has deepened, and many of the players have become more dangerous as we have become increasingly vulnerable. We are still seeing hack after hack and breach after breach. We hear about it daily in the news.

The more we shift to the internet as the conduit and the repository for everything we use and share and manage, the more danger we are in.

Today we are worried about a wider-than-ever range of threat actors, from multinational cyber syndicates to nation-state adversaries. And we are concerned about a wider-than-ever gamut of methods continually employed in new ways, like the targeting of managed service providers—MSPs—as a way to access scores of victims by hacking just one provider.

China's Ministry of State Security (MSS) pioneered that technique and, as you saw in July, we indicted two Chinese hackers who worked with the Guangdong State Security Department of the MSS. These individuals conducted a hacking campaign lasting more than 10 years, targeting countries with high technology industries, to include the United States. The industries targeted included, among others, solar energy, pharmaceuticals, and defense.

Cyber crimes like these, directed by the Chinese government's intelligence services, threaten not only the United States but also every other country that supports fair play, international norms, and the rule of law, and they also seriously undermine China's desire to become a respected leader in world affairs.

Theft of intellectual property is not the only cyber threat presented by the People's Republic of China (PRC) government. They are also working to obtain controlled defense technology and developing the ability to use cyber means to complement any future real-world conflict. All of them, and others, are working to simultaneously strengthen themselves and weaken the United States. And we are taking all these nation-state threats very seriously.

But as dangerous as nation-states are, we do not have the luxury of focusing on them alone. We also are battling the increasing sophistication of criminal groups that place many hackers on a level we used to see only among hackers working for governments.

The proliferation of malware as a service, where darkweb vendors sell sophistication in exchange for cryptocurrency, increases the difficulty of stopping what would once have been less-dangerous offenders. It can give a ring of unsophisticated criminals the tools to paralyze entire hospitals, police departments, and businesses with ransomware. Often the hackers themselves have not become much more sophisticated—but they are renting sophisticated capabilities, requiring us to up our game as we work to defeat them, too.

Hackers have not relented under the COVID-19 pandemic. On the contrary, they have attempted to compromise the computer systems of hospitals and medical centers to obtain patient financial data, medical records, and other information. In addition, such attacks on medical centers may lead to the interruption of computer networks and systems putting patients' lives at an increased risk when America faces its most dire health crisis in generations.

Conclusion

Chairman Thompson, Ranking Member Rogers and members of the committee, thank you for the opportunity to testify today. I am now happy to answer any questions you might have.

Number 3

About the Standard-Setting Process

PCAOB
Public Company Accounting Oversight Board

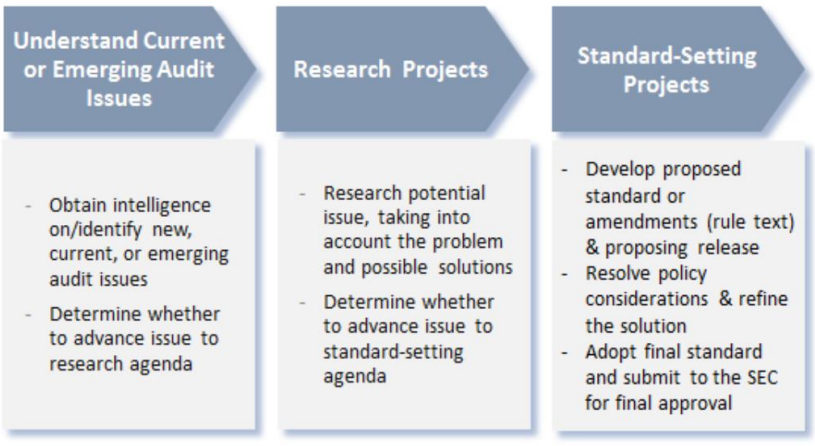
The PCAOB seeks to establish and maintain high quality auditing and related professional practice standards for audits of public companies and other issuers, and broker-dealers in support of the PCAOB mission to protect investors and further the public interest in the preparation of informative, accurate, and independent audit reports.

The PCAOB Office of the Chief Auditor — working with other PCAOB offices and divisions — assists the Board in establishing and maintaining PCAOB standards.

The PCAOB standard-setting activities include identifying current or emerging audit issues, developing the research agenda, and working on standard-setting projects.

These are informed by a range of activities, such as the PCAOB's oversight activities, consultation with the Standing Advisory Group, input from the Investor Advisory Group, discussion with SEC staff, the work of other standard setters (for example, the International Auditing and Assurance Standards Board, the Financial Accounting Standards Board, and the International Accounting Standards Board), and other relevant inputs and developments.

The PCAOB takes a priority-based approach to standard-related projects. The timing of each phase may vary from project to project, depending on the nature and scope of audit issues involved. A high level overview of the standard-setting process follows.



Understand Current or Emerging Audit Issues. The process begins with a PCAOB interdivisional team that performs an environmental scan to identify current or emerging audit issues and informs the Board about matters that potentially warrant changes to PCAOB standards or that warrant additional staff guidance.

The interdivisional team continues to monitor current or emerging issues, including observations from oversight activities, that may merit further consideration. The evaluation of potential issues may result in a project being added to the PCAOB research agenda.

Research Projects. For each research project, a PCAOB interdivisional research team is formed to perform research, outreach, and economic analysis to assess whether there is a need for changes to PCAOB standards; consider alternative regulatory responses; and, if standard setting is needed, evaluate the potential standard-setting scope and approaches.

If standard setting is pursued, the project would be added to the standard-setting agenda. If standard setting is not pursued, consideration would be given to whether any other action is needed. For example, the PCAOB staff may prepare guidance regarding the application of existing PCAOB standards.

In addition to the projects on the research agenda, the PCAOB also conducts monitoring activities in other areas that could impact audits or PCAOB standards (e.g., financial reporting fraud, auditor independence, and new accounting standards).

Standard-Setting Projects. For each standard-setting project, the PCAOB solicits public comment on potential changes to standards before adopting changes. Consideration of changes to standards also involves conducting an economic analysis and analyzing the potential impact of changes on audits of emerging growth companies.

Staff Guidance on Economic Analysis in PCAOB Standard Setting (Feb. 14, 2014), was prepared to provide guidance to PCAOB staff involved in rulemaking.

You may visit:
https://pcaobus.org/Standards/pages/05152014_guidance.aspx

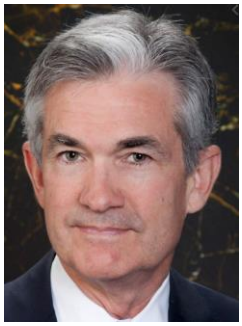
After the Board adopts changes to its standards, the changes must be approved by the SEC to become effective.

Further information about the PCAOB's projects may be found at Research and Standard-Setting Projects. The descriptions of these projects posted on our website are prepared by the staff of the Office of the Chief Auditor, and are not statements of the PCAOB, nor do they necessarily reflect the views of the Board, individual Board members, or other staff.

Number 4

Coronavirus Aid, Relief and Economic Security Act

Jerome H Powell, Chair of the Board of Governors of the Federal Reserve System, before the Committee on Financial Services, US House of Representatives, Washington DC.



Chairwoman Waters, Ranking Member McHenry, and other members of the Committee, thank you for the opportunity to update you on our ongoing measures to address the hardship wrought by the pandemic.

The Federal Reserve, along with others across government, is working to alleviate the economic fallout. We remain committed to using our tools to do what we can, for as long as it takes, to ensure that the recovery will be as strong as possible, and to limit lasting damage to the economy.

Economic activity has picked up from its depressed second-quarter level, when much of the economy was shut down to stem the spread of the virus. Many economic indicators show marked improvement.

Household spending looks to have recovered about three-fourths of its earlier decline, likely owing in part to federal stimulus payments and expanded unemployment benefits.

The housing sector has rebounded, and business fixed investment shows signs of improvement. In the labor market, roughly half of the 22 million payroll jobs that were lost in March and April have been regained as people return to work.

Both employment and overall economic activity, however, remain well below their pre-pandemic levels, and the path ahead continues to be highly uncertain. The downturn has not fallen equally on all Americans; those least able to bear the burden have been the most affected.

The rise in joblessness has been especially severe for lower-wage workers, for women, and for African-Americans and Hispanics. This reversal of economic fortune has upended many lives and created great uncertainty about the future.

A full recovery is likely to come only when people are confident that it is safe to reengage in a broad range of activities. The path forward will depend on keeping the virus under control, and on policy actions taken at all levels of government.

Since mid-March, we have taken forceful action, implementing a policy of near-zero rates, increasing asset holdings, and standing up 13 emergency lending facilities. We took these measures to support broader financial conditions and more directly support the flow of credit to households, businesses of all sizes, and state and local governments.

Our actions, taken together, have helped unlock more than $1 trillion of funding, which, in turn, has helped keep organizations from shuttering, putting them in a better position to keep workers on and to hire them back as the economy continues to recover.

The Main Street Lending Program (Main Street) has been of significant interest to this Committee and to the public. Many of the businesses affected by the pandemic are smaller firms that rely on banks for loans, rather than public credit markets. Main Street is designed to facilitate the flow of credit to small and medium-sized businesses.

In establishing the facility, we conducted extensive outreach, soliciting public comment and holding in-depth discussions with lenders and borrowers of all sizes.

In response to feedback, we have continued to make adjustments to Main Street to provide greater support to small and medium-sized businesses and to nonprofit organizations such as educational institutions, hospitals, and social service organizations.

Nearly 600 banks, representing well more than half of the assets in the banking system, have either completed registration or are in the process of doing so.

About 230 loans totaling roughly $2 billion are either funded or in the pipeline.

Main Street is intended for businesses that were on a sound footing pre-pandemic and that have good longer-term prospects but which have encountered temporary cash flow problems due to the pandemic and are not able to get credit on reasonable terms as a result.

Main Street loans may not be the right solution for some businesses, in part because the CARES Act states clearly that these loans cannot be forgiven.

Our credit facilities have improved lending conditions broadly, including for potential Main Street borrowers. The evidence suggests that most creditworthy small and medium-sized businesses can currently get loans from private-sector financial institutions.

Many of our programs rely on emergency lending powers that require the support of the Treasury Department and are available only in unusual circumstances. By serving as a backstop to key credit markets, our programs have significantly increased the extension of credit from private lenders.

However, the facilities are only that-a backstop. They are designed to support the functioning of private markets, not to replace them. Moreover, these are lending, not spending powers.

Many borrowers will benefit from these programs, as will the overall economy, but for others, a loan that could be difficult to repay might not be the answer. In these cases, direct fiscal support may be needed.

Our economy will recover fully from this difficult period. We remain committed to using our full range of tools to support the economy for as long as is needed.

Thank you. I look forward to your questions.

Summary of Section 13(3) Facilities Using CARES Act Funding
The Municipal Liquidity Facility

The Municipal Liquidity Facility (MLF) helps state and local governments better manage the extraordinary cash flow pressures associated with the pandemic, in which expenses, often for critical services, are temporarily higher than normal and tax revenues are delayed or temporarily lower than normal.

This facility addresses these liquidity needs by purchasing the short-term notes typically used by these governments, along with other eligible public entities, to manage their cash flows. By addressing the cash management needs of eligible issuers, the MLF was also intended to encourage private investors to reengage in the municipal securities market, including across longer maturities, thus supporting overall municipal market functioning.

Under the MLF, the Federal Reserve Bank of New York lends to a special purpose vehicle (SPV) that will directly purchase up to $500 billion of short-term notes issued by a range of eligible state and local government entities. Generally speaking, eligible issuers include all U.S. states, counties

with a population of at least 500,000 residents, cities with a population of at least 250,000 residents, certain multistate entities, and revenue-bond issuers designated as eligible issuers by their state governors.

Notes purchased by the facility carry yields designed to promote private market participation—that is, they carry fixed spreads based on the long-term rating of the issuer that are generally larger than those seen in normal times. With funding from the CARES Act (Coronavirus Aid, Relief and Economic Security Act), the Department of the Treasury has committed to make a $35 billion equity investment in the SPV.

As of September 18, the facility had purchased two issues for a total outstanding amount of $1.7 billion.

The MLF has contributed to a strong recovery in municipal securities markets, which has facilitated a historic issuance of more than $250 billion of bonds since late March.

State and local governments and other municipal bond issuers of a wide spectrum of types, sizes, and ratings have been able to issue bonds, including long maturity bonds, with interest rates that are at or near historical lows. Those municipal issuers who do not have direct access to the Federal Reserve under the MLF have still benefited substantially from a better-functioning municipal securities market.

To read more:
https://www.bis.org/review/r200922a.htm

Number 5

Promoting the soundness and efficiency of our insurance sector - recommencing the IPSA and Solvency Standard review

Geoff Bascand, Deputy Governor and General Manager of Financial Stability of the Reserve Bank of New Zealand, to the Insurance Council of New Zealand, Wellington.

RESERVE BANK OF NEW ZEALAND
TE PŪTEA MATUA

Introduction

Back in March, I was ready, speech in hand, to provide you all with an insurance update, particularly in relation to our plans for the review of the Insurance (Prudential Supervision) Act, or IPSA, that we started in 2017.

As with many things, COVID-19 intervened. My pandemic insurance was I could always do it later! As I update this speech, different alert level requirements are in place.

Again, just like many things I'm contemplating whether I might have to defer again, or do it differently – can one get insurance for multiple, repeated and arguably expected phenomena?

To some degree, this story is a metaphor for the IPSA review.

We have started and stopped it a couple of times, due to competing priorities for us and industry. We are now recommencing it.

We are confident we can do so sustainably, even with pandemic risks surrounding us.

The IPSA and associated Solvency Standard review, including our approach to the review and its timetable, are the main focus of my address today.

I'll also provide feedback on our view of the insurance sector's handling of the pandemic so far, as well as an update on the Appointed Actuary Thematic Review, some comments on issues that were significant before COVID-19 and remain in play, and an update on our supervisory approach, including our Auckland presence.

Before coming to the details of the IPSA Review, I want to remark on the importance of insurance and its place in our financial system.

Our insurance markets

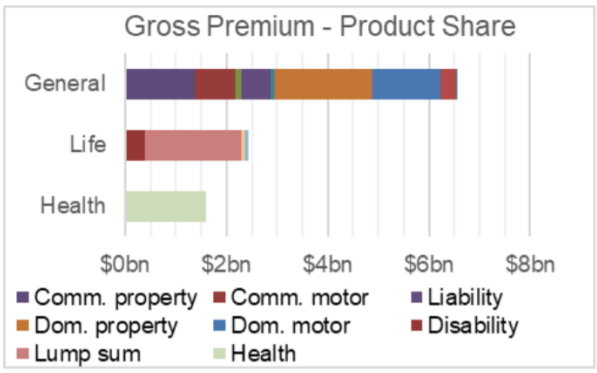
Maintaining a sound and efficient insurance sector is important for New Zealand. Customers are used to being able to insure their homes and possessions and obtain life and disability insurance, and businesses utilise a range of insurance products to protect their assets and business interruption exposures.

There are about 90 licensed insurers operating in New Zealand. The sector is highly diverse, ranging from large international companies to tiny specialised entities providing services to particular employee or professional groups.

The sector covers home and contents, motor vehicle, travel, life, health, disability, credit, income protection, business interruption, and other products or services. General insurance is the largest sector accounting for 63% of total premiums with life insurance representing 22% and health insurance 14%.

The distribution of gross premium between classes of insurance and between insurers is shown in Table 1.

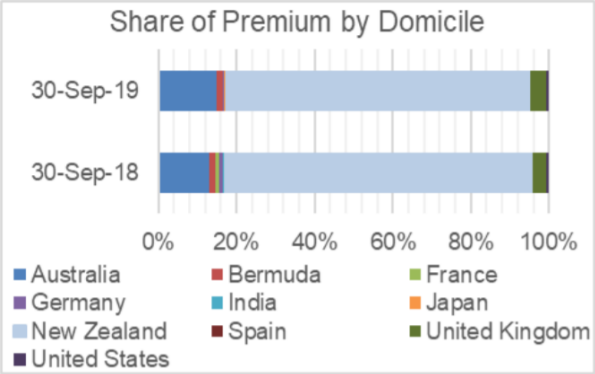
Table 1 - Insurers by size and sector[2]



IPSA's treatment of overseas insurers recognises that New Zealand is heavily reliant on foreign-based and foreign-owned life and general insurers.

Foreign-owned insurers include insurers operating in New Zealand as locally incorporated subsidiaries of overseas parents and insurers operating as branches.

Table 2 – Share of premium by country of incorporation of insurer[3]



[2] Quarterly Insurer Survey and Insurer Return
[3] Quarterly Insurer Survey and Insurer Return

IPSA provides for some exemptions to insurers operating as branches, providing their home regulator has been approved as meeting IPSA equivalence.

Table 2 shows the mix between locally incorporated insurers, which include subsidiaries of overseas insurers, and branches.

Regulatory equivalence between overseas domiciled insurers and locally incorporated insurers is important because customers should be able to regard their insurance product as trustworthy wherever the insurer is based.

Insurance isn't very useful if it can't be relied upon for pay-out when a claim is made, and our insurance market won't be efficient or serve New Zealanders well if we have unequal treatment of domestic and foreign insurers.

We want to see insurance remain available and affordable. Widely held property insurance helps manage the social and economic cost of natural hazard events for property owners and communities.

It also lowers the potential fiscal costs for the government to facilitate recovery.

Property insurance also has wider economic benefits by providing the confidence necessary for economic activity and investment, such as banks requiring evidence of insurance coverage to lend against properties.

Similar benefits exist in other forms of insurance - such as life and disability insurance - that support the willingness of individuals and businesses to take risks and protect them from financial hardship.

The Canterbury earthquakes revealed high levels of insurance penetration for home insurance in New Zealand.

The interaction between private insurance and the Earthquake Commission has also led to some changes and others continue to be reviewed in relation to EQC and insurers.

While there were low levels of non-insurance amongst homeowners, the risk of under-insurance was mitigated because most home insurance was provided on a total replacement basis.

Industry experience in managing home insurance claims without a cap on the rebuilding cost led to a change to sum insured policies that cover a specified dollar amount for rebuilding cost.

This development changes, to some degree, the allocation of risk between insurers, customers and the state.

The risk of underestimating rebuilding costs and having a sum insured that is too low has transferred from the insurer to their customers and, in turn, creates potential for increased economic risks if a significant number of homes cannot be rebuilt because pay-outs do not cover the full rebuild costs.

Life insurers in New Zealand have moved away from offering combined savings and insurance products and the market now primarily offers cover for pure risks, such as premature death, disability and sickness.

In doing so, insurance provides families with financial security to preserve financial assets and businesses with financial security to protect key personnel and the interests of owners.

To read more:
https://www.bis.org/review/r200918c.pdf

Number 6

Tip & Referral Center
Enforcement Tips, Referrals, Complaints, and Other Information

PCAOB
Public Company Accounting Oversight Board

Tips, referrals and other information from the public are important sources for the PCAOB. You can use this website to report potential violations of law or PCAOB rules, including self-reporting. The PCAOB enforcement staff will review your information promptly.

The Board appreciates any information you can provide that assists us in carrying out our public mission to protect the interests of investors through the oversight of auditors of public companies and broker-dealers.

Please contact us with information on any matter relating to PCAOB oversight, our regulatory responsibilities under the Sarbanes-Oxley Act of 2002, and the public accounting firms that we oversee.

For example, you may:

- File a complaint or provide a tip or referral on potential violations of law or PCAOB rules by a registered public accounting firm or people associated with the firm;

- Provide information that may be relevant to a PCAOB inspection of a public accounting firm or people associated with the firm;

- Provide any information that is relevant to the oversight responsibilities of the PCAOB.

What Happens to the Information You Submit

Enforcement staff immediately review and evaluate the information you provide. The PCAOB may use the information in inspections, investigations, or other Board activities. We also may provide the information to state or federal regulatory or law enforcement agencies, or foreign authorities, as appropriate.

Federal law prohibits the PCAOB and its staff from disclosing information about the Board's investigative and enforcement activities, unless and until the information results in a public proceeding. For this reason, we may not be able to share with you information on action we take to follow up on your tip.

To Submit a Tip, Referral, or Other Information

You can reach us by email, fax, telephone or postal mail.

Online: Tip & Referral Form (https://pcaobus.org/Enforcement/Tips/Pages/TipsForm.aspx)

Please describe the activity or transaction that is of concern to you and describe the facts and circumstances you wish to bring to the attention of the PCAOB:

To assist us in understanding the nature of your concerns, please check all boxes that apply:

Auditor Concerns:

- ☐ **Auditor Independence**
- ☐ **Auditor Ethics**
- ☐ **Auditor's Quality Control System**
- ☐ **Audit Standards**
- ☐ **Auditor's Review of Interim Financial Statements**
- ☐ **Document Destruction**
- ☐ **Fraud**
- ☐ **GAAP Issues**

Email: Tip & Referral Center

Fax: 202-862-0757

Phone: 800-741-3158 (Leave a message)

Postal Mail: PCAOB Tip & Referral Center, 1666 K Street NW, Washington, DC 20006

Number 7

BIS Statistics: Charts

BIS Quarterly Review, September 2020, International banking and financial market developments

The statistics published by the BIS are a unique source of information about the structure of and activity in the global financial system. BIS statistics are presented in graphical form in this annex and in tabular form in the BIS Statistical Bulletin, which is published concurrently with the BIS Quarterly Review.

For introductions to the BIS statistics and a glossary of terms used in this annex, see the BIS Statistical Bulletin. The data shown in the charts in this annex can be downloaded from the BIS Quarterly Review page on the BIS website (www.bis.org/publ/quarterly.htm).

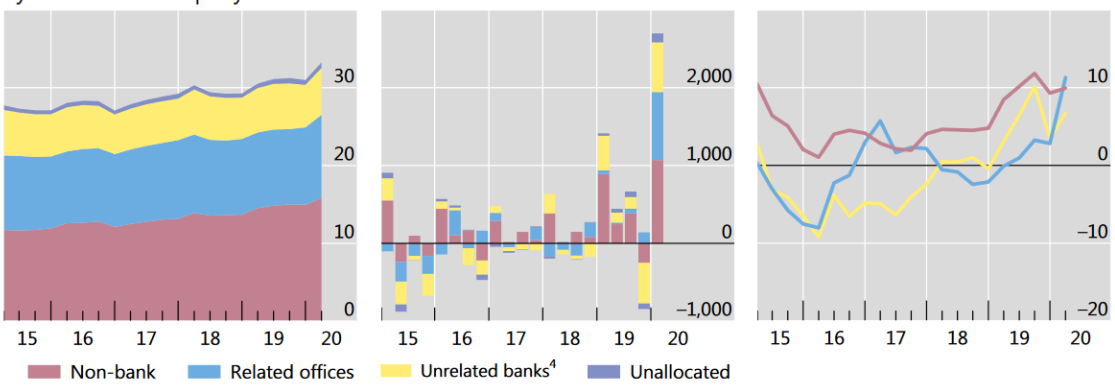
Data may have been revised or updated subsequent to the publication of this annex.

For the latest data and to download additional data, see the statistics pages on the BIS website (www.bis.org/statistics/index.htm).

A release calendar provides advance notice of publication dates (www.bis.org/statistics/relcal.htm)

You may visit page 83 at: https://www.bis.org/publ/qtrpdf/r_qt2009.pdf

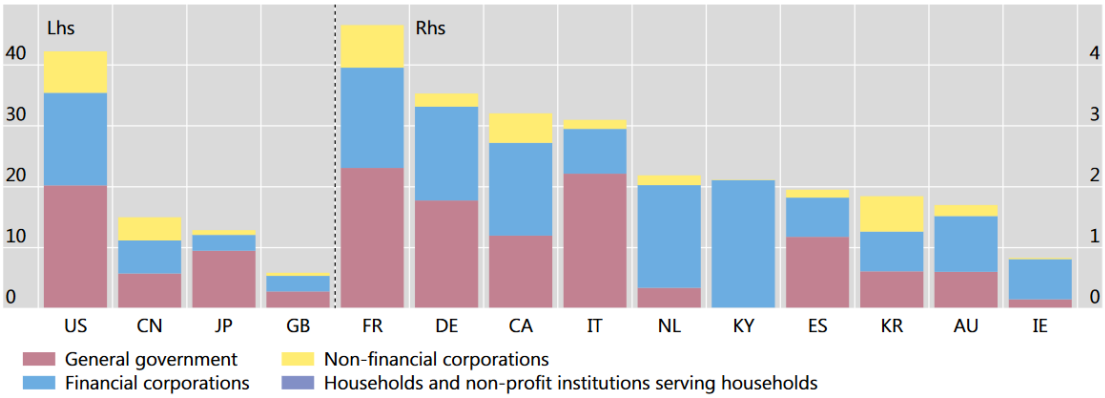
Cross-border claims, by sector, currency and instrument — Graph A.1



Total debt securities, by residence and sector of issuer[1]

Amounts outstanding for the latest available data, in trillions of US dollars[2]

Graph C.2



Further information on the BIS debt securities statistics is available at www.bis.org/statistics/secstats.htm.

[1] For countries that do not report TDS, data are estimated by the BIS as DDS plus IDS. [2] Amounts denominated in currencies other than the US dollar are converted to US dollars at the exchange rate prevailing on the reference date.

Sources: National data; BIS debt securities statistics.

Number 8

UEFI Secure Boot Customization

National Security Agency, Cybersecurity Technical Report

Secure Boot is a boot integrity feature that is part of the Unified Extensible Firmware Interface (UEFI) industry standard.

Most modern computer systems are delivered to customers with a standard Secure Boot policy installed.

This document provides a comprehensive guide for customizing a Secure Boot policy to meet several use cases.

UEFI is a replacement for the legacy Basic Input Output System (BIOS) boot mechanism.

UEFI provides an environment common to different computing architectures and platforms.

UEFI also provides more configuration options, improved performance, enhanced interfaces, security measures to combat persistent firmware threats, and support for a wider variety of devices and form factors.

Malicious actors target firmware to persist on an endpoint.

Firmware is stored and executes from memory that is separate from the operating system and storage media.

Antivirus software, which runs after the operating system has loaded, is ineffective at detecting and remediating malware in the early-boot firmware environment that executes before the operating system.

Secure Boot provides a validation mechanism that reduces the risk of successful firmware exploitation and mitigates many published early-boot vulnerabilities.

Secure Boot is frequently not enabled due to issues with incompatible hardware and software. Custom certificates, signatures, and hashes should be utilized for incompatible software and hardware.

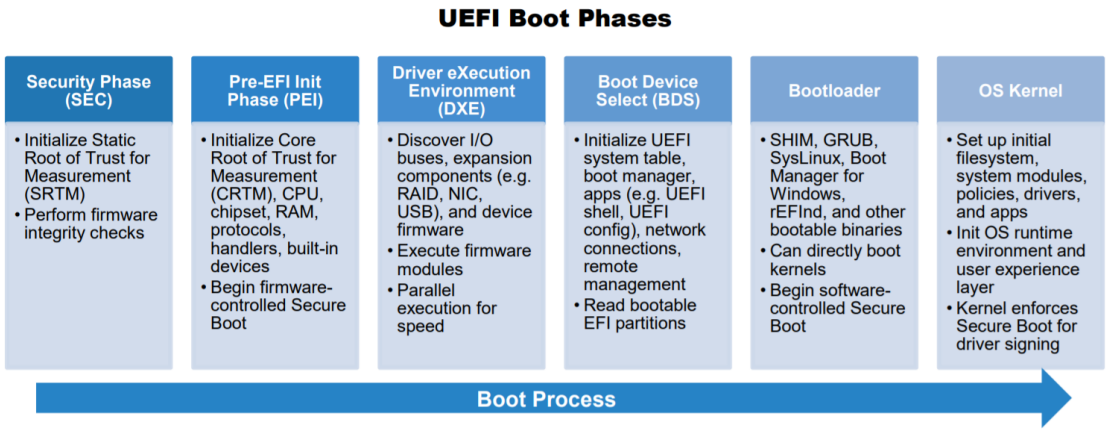


Figure 1 - An enumeration of UEFI firmware and software boot phases.

Secure Boot can be customized to meet the needs of different environments.

Customization enables administrators to realize the benefits of boot malware defenses, insider threat mitigations, and data-at-rest protections.

Administrators should opt to customize Secure Boot rather than disable it for compatibility reasons.

Customization may – depending on implementation – require infrastructures to sign their own boot binaries and drivers.

Recommendations for system administrators and infrastructure owners:

• Machines running legacy BIOS or Compatibility Support Module (CSM) should be migrated to UEFI native mode.

• Secure Boot should be enabled on all endpoints and configured to audit firmware modules, expansion devices, and bootable OS images (sometimes referred to as Thorough Mode).

• Secure Boot should be customized, if necessary, to meet the needs of organizations and their supporting hardware and software.

• Firmware should be secured using a set of administrator passwords appropriate for a device's capabilities and use case.

• Firmware should be updated regularly and treated as importantly as operating system and application updates.

• A Trusted Platform Module (TPM) should be leveraged to check the integrity of firmware and the Secure Boot configuration.

To read more:
https://media.defense.gov/2020/Sep/15/2002497594/-1/-1/0/CTR-UEFI-SECURE-BOOT-CUSTOMIZATION-20200915.PDF/CTR-UEFI-SECURE-BOOT-CUSTOMIZATION-20200915.PDF

Number 9

New cyberattacks targeting U.S. elections

Tom Burt - Corporate Vice President, Customer Security & Trust

Microsoft

In recent weeks, Microsoft has detected cyberattacks targeting people and organizations involved in the upcoming presidential election, including unsuccessful attacks on people associated with both the Trump and Biden campaigns, as detailed below.

We have and will continue to defend our democracy against these attacks through notifications of such activity to impacted customers, security features in our products and services, and legal and technical disruptions.

The activity we are announcing today makes clear that foreign activity groups have stepped up their efforts targeting the 2020 election as had been anticipated, and is consistent with what the U.S. government and others have reported.

We also report here on attacks against other institutions and enterprises worldwide that reflect similar adversary activity.

We have observed that:

- Strontium, operating from Russia, has attacked more than 200 organizations including political campaigns, advocacy groups, parties and political consultants

- Zirconium, operating from China, has attacked high-profile individuals associated with the election, including people associated with the Joe Biden for President campaign and prominent leaders in the international affairs community

- Phosphorus, operating from Iran, has continued to attack the personal accounts of people associated with the Donald J. Trump for President campaign

The majority of these attacks were detected and stopped by security tools built into our products.

We have directly notified those who were targeted or compromised so they can take action to protect themselves. We are sharing more about the details of these attacks today, and where we've named impacted customers, we're doing so with their support.

What we've seen is consistent with previous attack patterns that not only target candidates and campaign staffers but also those they consult on key issues.

These activities highlight the need for people and organizations involved in the political process to take advantage of free and low-cost security tools to protect themselves as we get closer to election day.

At Microsoft, for example, we offer AccountGuard threat monitoring, Microsoft 365 for Campaigns and Election Security Advisors to help secure campaigns and their volunteers.

More broadly, these attacks underscore the continued importance of work underway at the United Nations to protect cyberspace and initiatives like the Paris Call for Trust and Security in Cyberspace.

Strontium

Strontium is an activity group operating from Russia whose activities Microsoft has tracked and taken action to disrupt on several previous occasions.

It was also identified in the Mueller report as the organization primary responsible for the attacks on the Democratic presidential campaign in 2016.

Microsoft's Threat Intelligence Center (MSTIC) has observed a series of attacks conducted by Strontium between September 2019 and today.

Similar to what we observed in 2016, Strontium is launching campaigns to harvest people's log-in credentials or compromise their accounts, presumably to aid in intelligence gathering or disruption operations.

Many of Strontium's targets in this campaign, which has affected more than 200 organizations in total, are directly or indirectly affiliated with the upcoming U.S. election as well as political and policy-related organizations in Europe.

These targets include:

- U.S.-based consultants serving Republicans and Democrats;

- Think tanks such as The German Marshall Fund of the United States and advocacy organizations;

- National and state party organizations in the U.S.; and

- The European People's Party and political parties in the UK.

Others that Strontium targeted recently include businesses in the entertainment, hospitality, manufacturing, financial services and physical security industries.

Microsoft has been monitoring these attacks and notifying targeted customers for several months, but only recently reached a point in our investigation where we can attribute the activity to Strontium with high confidence.

MSTIC's investigation revealed that Strontium has evolved its tactics since the 2016 election to include new reconnaissance tools and new techniques to obfuscate their operations.

In 2016, the group primarily relied on spear phishing to capture people's credentials.

In recent months, it has engaged in brute force attacks and password spray, two tactics that have likely allowed them to automate aspects of their operations.

Strontium also disguised these credential harvesting attacks in new ways, running them through more than 1,000 constantly rotating IP addresses, many associated with the Tor anonymizing service.

Strontium even evolved its infrastructure over time, adding and removing about 20 IPs per day to further mask its activity.

We are also working with our customers to assist them in proactively hunting for these types of threats in their environments and have published additional detail and guidance on Strontium activity.

You may visit:
https://www.microsoft.com/security/blog/2020/09/10/strontium-detecting-new-patters-credential-harvesting/

Zirconium

Zirconium, operating from China, has attempted to gain intelligence on organizations associated with the upcoming U.S. presidential election.

We've detected thousands of attacks from Zirconium between March 2020 and September 2020 resulting in nearly 150 compromises. Its targets have included individuals in two categories.

First, the group is targeting people closely associated with U.S. presidential campaigns and candidates.

For example, it appears to have indirectly and unsuccessfully targeted the Joe Biden for President campaign through non-campaign email accounts belonging to people affiliated with the campaign.

The group has also targeted at least one prominent individual formerly associated with the Trump Administration.

Second, the group is targeting prominent individuals in the international affairs community, academics in international affairs from more than 15 universities, and accounts tied to 18 international affairs and policy organizations including the Atlantic Council and the Stimson Center.

Zirconium is using what are referred to as web bugs, or web beacons, tied to a domain they purchased and populated with content. The actor then sends the associated URL in either email text or an attachment to a targeted account.

Although the domain itself may not have malicious content, the web bug allows Zirconium to check if a user attempted to access the site. For nation-state actors, this is a simple way to perform reconnaissance on targeted accounts to determine if the account is valid or the user is active.

Phosphorus

Phosphorus is an activity group operating from Iran that MSTIC has tracked extensively for several years.

The actor has operated espionage campaigns targeting a wide variety of organizations traditionally tied to geopolitical, economic or human rights interests in the Middle East region.

Microsoft has previously taken legal action against Phosphorus' infrastructure and its efforts late last year to target a U.S. presidential campaign.

Last month, as part of our ongoing efforts to disrupt Phosphorus activity, Microsoft was again given permission by a federal court in Washington D.C. to take control of 25 new internet domains used by the Phosphorus.

Microsoft has since taken control of these domains.

To date, we have used this method to take control of 155 Phosphorus domains.

Since our last disclosure, Phosphorus has attempted to access the personal or work accounts of individuals involved directly or indirectly with the U.S. presidential election.

Between May and June 2020, Phosphorus unsuccessfully attempted to log into the accounts of administration officials and Donald J. Trump for President campaign staff.

Bolstering Cybersecurity

We disclose attacks like these because we believe it's important the world knows about threats to democratic processes.

It is critical that everyone involved in democratic processes around the world, both directly or indirectly, be aware of these threats and take steps to protect themselves in both their personal and professional capacities.

We report on nation-state activity to our customers and more broadly when material to the public, regardless of the actor's nation-state affiliation.

We are taking extra steps to protect customers involved in elections, government and policymaking.

We'll continue to disclose additional significant activity in our efforts to defend democracy.

We also believe more federal funding is needed in the U.S. so states can better protect their election infrastructure.

While the political organizations targeted in attacks from these actors are not those that maintain or operate voting systems, this increased activity related to the U.S. electoral process is concerning for the whole ecosystem.

We continue to encourage state and local election authorities in the U.S. to harden their operations and prepare for potential attacks.

But as election security experts have noted, additional funding is still needed, especially as resources are stretched to accommodate the shift in COVID-19-related voting.

We encourage Congress to move forward with additional funding to the states and provide them with what they need to protect the vote and ultimately our democracy.

Number 10

Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally

Two Defendants Arrested in Malaysia; Remaining Five Defendants, One of Whom Allegedly Boasted of Connections to the Chinese Ministry of State Security, are Fugitives in China

THE UNITED STATES DEPARTMENT of JUSTICE

In August 2019 and August 2020, a federal grand jury in Washington, D.C., returned two separate indictments charging five computer hackers, all of whom were residents and nationals of the People's Republic of China (PRC), with computer intrusions affecting over 100 victim companies in the United States and abroad, including software development companies, computer hardware manufacturers, telecommunications providers, social media companies, video game companies, non-profit organizations, universities, think tanks, and foreign governments, as well as pro-democracy politicians and activists in Hong Kong.

The intrusions, which security researchers have tracked using the threat labels "APT41," "Barium," "Winnti," "Wicked Panda," and "Wicked Spider," facilitated the theft of source code, software code signing certificates, customer account data, and valuable business information.

These intrusions also facilitated the defendants' other criminal schemes, including ransomware and "crypto-jacking" schemes, the latter of which refers to the group's unauthorized use of victim computers to "mine" cryptocurrency.

Also in August 2020, the same federal grand jury returned a third indictment charging two Malaysian businessmen who conspired with two of the Chinese hackers to profit from computer intrusions targeting the video game industry in the United States and abroad.

Shortly thereafter, the U.S. District Court for the District of Columbia issued arrest warrants for the two businessmen.

On Sept. 14, 2020, pursuant to a provisional arrest request from the United States with a view to their extradition, Malaysian authorities arrested them in Sitiawan. The department appreciates the significant cooperation and assistance provided by the Government of Malaysia, including the Attorney General's Chambers of Malaysia and the Royal Malaysia Police.

In addition to arrest warrants for all of the charged defendants, in September 2020, the U.S. District Court for the District of Columbia issued seizure warrants that resulted in the recent seizure of hundreds of accounts, servers, domain names, and command-and-control (C2") "dead drop" web pages used by the defendants to conduct their computer intrusion offenses.

The FBI executed the warrants in coordination with other actions by several private-sector companies, which included disabling numerous accounts for violations of the companies' terms of service. In addition, in partnership with the department, Microsoft developed and implemented technical measures to block this threat actor from accessing victims' computer systems.

The actions by Microsoft were a significant part of the overall effort to deny the defendants continued access to hacking infrastructure, tools, accounts, and command and control domain names. In coordination with today's announcement, the FBI has also released a Liaison Alert System (FLASH) report that contains critical, relevant technical information collected by the FBI for use by specific private-sector partners.

"The department of Justice has used every tool available to disrupt the illegal computer intrusions and cyberattacks by these Chinese citizens," said Deputy Attorney General Jeffrey A. Rosen. "Regrettably, the Chinese communist party has chosen a different path of making China safe for cybercriminals so long as they attack computers outside China and steal intellectual property helpful to China."

"Today's charges, the related arrests, seizures of malware and other infrastructure used to conduct intrusions, and coordinated private sector protective actions reveal yet again the department's determination to use all of the tools at its disposal and to collaborate with the private sector and nations who support the rule of law in cyberspace," said Assistant Attorney General John C. Demers. "This is the only way to neutralize malicious nation state cyber activity."

"Today's announcement demonstrates the ramifications faced by the hackers in China but it is also a reminder to those who continue to deploy malicious cyber tactics that we will utilize every tool we have to administer justice," said FBI Deputy Director David Bowdich. "The arrests in Malaysia are a direct result of partnership, cooperation and collaboration. As the cyber threat continues to evolve larger than any one agency can address, the FBI remains committed to being an indispensable partner to our federal, international and private sector partners to stop rampant cyber crime and hold those carrying out these kind of actions accountable."

"The scope and sophistication of the crimes in these unsealed indictments is unprecedented. The alleged criminal scheme used actors in China and Malaysia to illegally hack, intrude and steal information from victims worldwide," said Michael R. Sherwin, Acting U.S. Attorney for the District of Columbia. "As set forth in the charging documents, some of these criminal actors believed their association with the PRC provided them free license to hack and steal across the globe. This scheme also contained a new and troubling cyber-criminal component – the targeting and utilization of gaming platforms to both defraud video game companies and launder illicit proceeds."

"The actions announced today reflect a years-long commitment by the FBI Washington Field Office to pursue the perpetrators of the computer intrusion campaigns described in the indictments, and to bring those perpetrators to justice," said Acting Assistant Director in Charge James A. Dawson, FBI Washington Field Office. "This case demonstrates the FBI's dedication to pursuing these criminals no matter where they are, and to whom they may be connected."

The August 2019 indictment charged Zhang Haoran, 35, and Tan Dailin, 35, with 25 counts of conspiracy, wire fraud, aggravated identity theft, money laundering, and violations of the Computer Fraud and Abuse Act ("CFAA"). The indictment charged Zhang and Tan with participating in a "Computer Hacking Conspiracy," which targeted high-technology and similar organizations.

The indictment also charged that, as an additional way to make money, Zhang and Tan participated in a "Video Game Conspiracy," through which Zhang and Tan, together with others, sought to make money by hacking video game companies, obtaining and otherwise generating digital items of value (e.g., video game currency), and then selling such items for profit.

In several instances, they used their unauthorized access to gaming company networks take action against other unrelated groups engaged in the same fraudulent generation of gaming artifacts, thereby attempting to eliminate the criminal competition.

One of the August 2020, indictments charged Jiang Lizhi, 35, Qian Chuan, 39, and Fu Qiang, 37, with nine counts of racketeering conspiracy, conspiracy to violate the CFAA, substantive violations of the CFAA, access device fraud, identity theft, aggravated identity theft, and money laundering.

The racketeering conspiracy pertained to the three defendants' conducting the affairs of Chengdu 404 Network Technology ("Chengdu 404"), a PRC

company, through a pattern of racketeering activity involving computer intrusion offenses affecting over 100 victim companies, organizations, and individuals in the United States and around the world, including in Australia, Brazil, Chile, Hong Kong, India, Indonesia, Japan, Malaysia, Pakistan, Singapore, South Korea, Taiwan, Thailand, and Vietnam.

The defendants also compromised foreign government computer networks in India and Vietnam, and targeted, but did not compromise, government computer networks in the United Kingdom.

In one notable instance, the defendants conducted a ransomware attack on the network of a non-profit organization dedicated to combating global poverty.

The defendants associated with Chengdu 404 employed sophisticated hacking techniques to gain and maintain access to victim computer networks. One example was the defendants' use of "supply chain attacks," in which the hackers compromised software providers and then modified the providers' code to facilitate further intrusions against the software providers' customers.

Another example was the hackers' use of C2 "dead drops," which are seemingly legitimate web pages that the hackers created, but which were surreptitiously encoded instructions to their malware. However, they also employed publicly available exploits and tools, including the following common vulnerabilities and exposures ("CVE"): CVE-2019-19781, CVE-2019-11510, CVE-2019-16920, CVE-2019-16278, CVE-2019-1652/CVE-2019-1653, and CVE-2020-10189.

The second August 2020 indictment charged Wong Ong Hua, 46, and Ling Yang Ching, 32, both Malaysian nationals and residents, with 23 counts of racketeering, conspiracy, identity theft, aggravated identity theft, access device fraud, money laundering, violations of the CFAA, and falsely registering domain names.

The indictment alleged that Wong and Ling conducted the affairs of Sea Gamer Mall, a Malaysian company founded by Wong, through a pattern of racketeering activity involving computer intrusion offenses targeting the video game industry in the United States, France, Japan, Singapore, and South Korea.

The indictment alleged that Wong and Ling worked with various hackers, including Zhang and Tan, to profit from the hackers' criminal computer intrusions at video game companies.

The indictment against Zhang and Tan charges the defendants with two counts of conspiracy to commit computer fraud, which carries a maximum sentence of five years in prison; two counts of conspiracy to commit wire fraud, which carries a maximum sentence of 20 years in prison; five counts of wire fraud, which carries a maximum sentence of 20 years in prison; nine counts of intentional damage to a protected computer, which carries a maximum sentence of 10 years in prison; four counts of unauthorized access to a protected computer, which carries a maximum sentence of five years in prison; two counts of aggravated identity theft, which carries a mandatory sentence of two years in prison; and one count of money laundering, which carries a maximum sentence of 20 years in prison.

The indictment against Jiang, Qian, and Fu charges the defendants with one count of racketeering conspiracy, which carries a maximum sentence of 20 years in prison; one count of conspiracy to commit computer fraud, which carries a maximum sentence of five years in prison; one count of intentional damage to a protected computer, which carries a maximum sentence of 10 years in prison; one count of unauthorized access to a protected computer, which carries a maximum sentence of five years in prison; one count of threatening to damage a protected computer, which carries a maximum sentence of five years in prison; one count of access device fraud, which carries a maximum sentence of 10 years in prison; one count of identity theft, which carries a maximum sentence of five years in prison; one count of aggravated identity theft, which carries a mandatory sentence of two years in prison; and one count of money laundering, which carries a maximum sentence of 20 years in prison.

The indictment against Wong and Ling charges the defendants with one count of racketeering conspiracy, which carries a maximum sentence of 20 years in prison; one count of racketeering, which carries a maximum sentence of 20 years in prison; three counts of intentional damage to a protected computer, which carries a maximum sentence of 10 years in prison; five counts of unauthorized access to a protected computer, which carries a maximum sentence of five years in prison; five counts of furthering fraud by unauthorized access to a protected computer, which carries a maximum sentence of five years in prison; two counts of access device fraud, which carries a maximum sentence of 10 years in prison; two counts of identity theft, which carries a maximum sentence of five years in prison; one count of aggravated identity theft, which carries a mandatory sentence of two years in prison; and three counts of money laundering, which carries a maximum sentence of 20 years in prison.

The indictment also alleges false registration of domain names, which would increase the maximum sentence of imprisonment for money laundering to 27 years; the maximum sentence of imprisonment for

unlawful access to a protected computer to 10 years instead of five years; the maximum sentence of imprisonment for intentional damage to a protected computer to 17 years instead of 10 years; and the mandatory sentence of imprisonment for aggravated identity theft to four years instead of two years.

The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only; any sentencing's of the defendants will be determined by the assigned judge.

The investigation was conducted jointly by the U.S. Attorney's Office for the District of Columbia, the National Security Division of the Department of Justice, and the FBI's Washington Field Office.

The FBI's Cyber Division assisted in the investigation and, along with FBI's Cyber Assistant Legal Attachés and Legal Attachés in countries around the world, provided essential support. Numerous victims cooperated and provided valuable assistance in the investigation.

The department is also grateful to Microsoft, including Microsoft's Threat Intelligence Center (MSTIC) and Digital Crimes Unit (DCU), to Google, including its Threat Analysis Group (TAG), to Facebook, and to Verizon Media, including its Paranoids Advanced Cyber Threats Team, for the assistance they provided in this investigation.

Assistant U.S. Attorney Demian Ahn of the District of Columbia, Assistant U.S. Attorney Tejpal Chawla of the District of Columbia, and Trial Attorney Evan Turgeon of the National Security Division's Counterintelligence and Export Control Section are prosecuting this case.

The Justice Department's Office of International Affairs provided critical assistance.

The details contained in the charging document are allegations. The defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

To read more:
https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any individual or entity;

- should not be relied on in the context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors.

However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

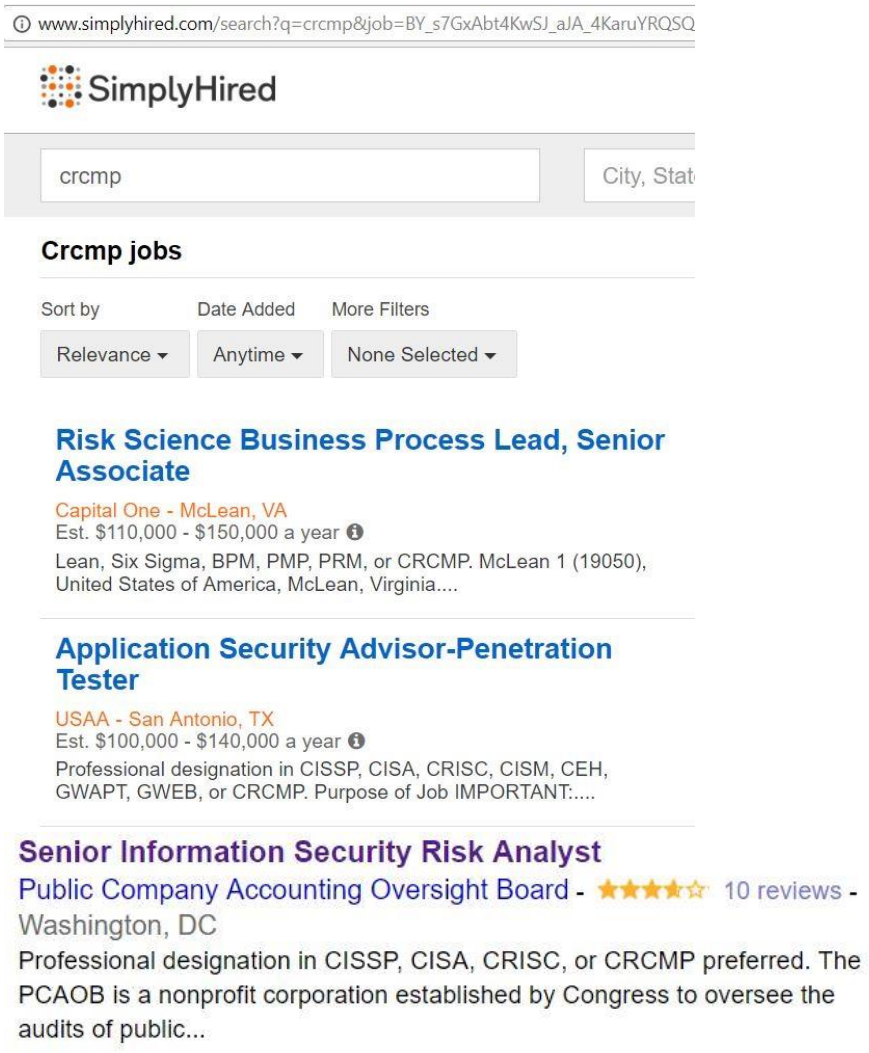
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

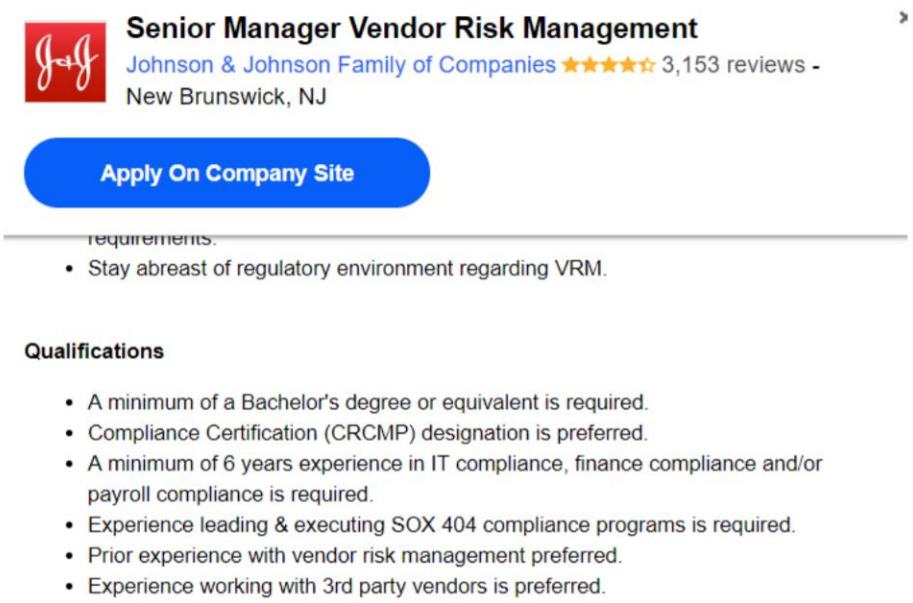
You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.
You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

2. *Weekly Updates* - Visit the *Reading Room* of the association at:
https://www.risk-compliance-association.com/Reading_Room.htm

3. *Training and Certification* – Become a Certified Risk and Compliance Management Professional (CRCMP), a Certified Information Systems Risk and Compliance Professional (CISRCP), a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, and / or a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I.





Senior Manager Vendor Risk Management

Johnson & Johnson Family of Companies ★★★★☆ 3,153 reviews -
New Brunswick, NJ

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

- A minimum of a Bachelor's degree or equivalent is required.
- Compliance Certification (CRCMP) designation is preferred.
- A minimum of 6 years experience in IT compliance, finance compliance and/or payroll compliance is required.
- Experience leading & executing SOX 404 compliance programs is required.
- Prior experience with vendor risk management preferred.
- Experience working with 3rd party vendors is preferred.

Companies and organizations like Accenture, American Express, USAA etc. consider the Certified Risk and Compliance Management Professional (CRCMP) program a preferred certificate. There are CRCMPs in 32 countries.

You can find more about the demand for CRCMPs at:
https://www.risk-compliance-association.com/CRCMP_Jobs_Careers.pdf

For the Certified Risk and Compliance Management Professional (CRCMP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

For the Certified Information Systems Risk and Compliance Professional (CISRCP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

For the Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm

For the Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CRCMP_Re_I.htm

For *instructor-led* training, you may contact us. We can tailor all programs to meet specific requirements.

4. *IARCP Authorized Certified Trainer (IARCP-ACT) Program* - This is an additional advantage on your resume, serving as a third-party endorsement to your knowledge and experience.

Certificates are important when being considered for a promotion or other career opportunities. You give the necessary assurance that you have the knowledge and skills to accept more responsibility.

To learn more, you may visit:
https://www.risk-compliance-association.com/IARCP_ACT.html

5. *Approved Training and Certification Centers (IARCP-ATCCs)* - In response to the increasing demand for CRCMP training, the International Association of Risk and Compliance Professionals is developing a world-wide network of Approved Training and Certification Centers (IARCP-ATCCs).

This will give the opportunity to risk and compliance managers, officers, and consultants to have access to instructor led training at convenient locations that meet international standards.

ATCCs use IARCP approved course materials and have access to IARCP Authorized Certified Trainers (IARCP-ACTs).

To learn more:
https://www.risk-compliance-association.com/Approved_Centers.html