TransReflections

Cyber Newsletter

March 2021

TransRe™
cyber
We value risk.

Table of Contents

Introduction

Welcome to our latest newsletter which arrives at a point of inflection in the cyber insurance market. In the second half of 2020, cyber insurance turned into a hardening market after a somewhat tepid start to the year. In parallel to other lines the rates gathered momentum as the year drew to a close. This was largely results driven with the deterioration in loss ratios becoming immediately apparent in 2019 and 2020 and driven by ransomware claims. Consequently, rate increases are also now accompanied by revised underwriting strategy. For many cyber insurers 2019 is unlikely to be a profitable year. There are several ransomware and ensuing business interruption claims in the market in excess of $50M. The frequency of full limit primary losses has materially increased in the US and Europe. It is not just the short-tail aspect. We have also seen recent Biometric Information Privacy Act claims into the 2016 underwriting year. Not surprisingly there has been a shift in appetite on both the insurance and reinsurance side. In the cyber insurance market, there has been a retraction in capacity deployed and far greater focus on re-evaluated risk selection and ransomware strategies. Insurers continue to seek to transfer more risk into the reinsurance market. Reinsurers are grappling with increasing loss ratios and having to contemplate whether the intrusions into SolarWinds or Accellion will be impactful events to their portfolios.

The effectiveness of ransomware strategies remains unproven but there is now a huge amount of attention to this within insurers. Initial strategies to focus on the efficacy of offline back-ups were circumnavigated by the trend last year to exfiltrate data if ransoms were not paid. There is now more underwriting scrutiny on ensuring assureds are adhering to the security posture that they have declared in their application and making sure they continuously refine that stance to maintain best practice. We are also seeing more widespread engagement of 3rd party cyber security specialists to help weed out risks that will be overly susceptible to attack. This should help raise the overall bar in terms of the level of information that will be provided or that can be interrogated efficiently to assess risk.

The cyber insurance market has had some near misses with Wannacry and NotPetya having a mild impact on loss ratios. It is arguable that this lulled some participants into a false sense of profitability and unrealistic loss ratio assumptions. Either through inadequate allowance for a cat loading or via pointing to a missed loss on one of the large data breach claims as evidence of superior performance. As coverage expanded and pricing subsequently deteriorated perhaps the increase in ransomware claims has manifested itself at opportune time? Maybe it has afforded a chance to re-evaluate the scope of insurability before a huge cyber cat event causes far greater losses. There are positive signs that insurers are in a market where the tide is turning towards more widespread rigorous underwriting. Previous assumptions around SME sector profitability are being challenged. Now is the time that new technology and ideas can be embedded into the underwriting process without a fear that subsequent changes in risk appetite will have a detrimental impact on market share. Reinsurers are also benefiting from improved data and more meaningful discussions around systemic risk. After all, SolarWinds was not a name at the forefront of many reinsurers minds before December of last year.

We look forward to seeing positive results from the new ransomware strategies adopted. However, cyber insurance is not just about ransomware. While numerous threat vectors are unlikely to dissipate this year, we can be optimistic that this marketplace is striding to a more sustainable footing in 2021.

Rhett Hewitt
March 2021

Notable Breaches

FireEye Hacked – SolarWinds Breach Effects Government Security

In late 2020, FireEye a prominent cybersecurity firm announced they had been hacked by a highly sophisticated Nation-State hacker. The hackers gained access to FireEye's systems and their most advanced security tools. A few days after that announcement, SolarWinds, a cybersecurity firm that provides services to private companies and federal agencies was hacked using FireEye tools. SolarWinds had pushed out malware installed to its clients, resulting in breaches across an unknown number of US federal agencies, including the departments of State, Treasury, Commerce, Energy and Homeland Security. Multiple private companies were also breached. The full scope and ramifications of the breaches remain unclear.

Accellion Data Breach Impact Continues to Grow

In December 2020, Accellion a leading cloud provider was hacked and claimed it was a relatively minor event and all vulnerabilities were patched within 72 hours. The claim was later abandoned after additional vulnerabilities and unauthorized access was confirmed over a month later. 300+ companies may have been affected including major corporations, large universities and governmental agencies.

Blackbaud Ransomware Hack Has Far-Reaching Implications

In May 2020, international cloud services provider Blackbaud (focused in the non-profit space) was subject to a ransomware attack that affected a huge number of users. Affected customers were not notified until August 2020. Numerous lawsuits have already been filed against Blackbaud and its customers. Millions of people had banking information and other PII information compromised during the breach.

Garmin Suffers Ransomware Attack

Garmin has reportedly paid a multi-million dollar ransom to regain access to its systems after they were allegedly breached by Evil Corp., a hacking collective with ties to Russia. The ransom payment (which has not been confirmed) may attract attention from regulators as Evil Corp. is on the US sanctions list.

Alcohol Delivery Company Breached

In February 2020, Drizly was breached by hackers and the company did not notify the 2.5M customers who were compromised and had financial data stolen until July 2020. Lawyers for those who were affected have called Drizly "oblivious" after it took them so long to recognize the breach.

GWU Hospital and UVM Health Among Healthcare Entities Targeted by Cyberattack

In September 2020, the company that oversees George Washington University Hospital, Universal Health Services, was hit with a cyberattack that lasted for weeks and forced staff at multiple locations to return to offline record keeping. In October 2020, the attack on UVM Health Network lasted 40+ days and will cost $63M in response costs and damages. In the early stages of Covid-19, some cyber attackers stated they would not attack medical facilities during the pandemic. Those assertions have proved aspirational at best as a number of hospitals and healthcare facilities have been targeted, including one that triggered an FBI warning to the whole sector.

Death by Ransomware

In September 2020, Düsseldorf University Hospital experienced a ransomware attack that rendered their computer systems inoperable. A patient was scheduled to have a life-saving procedure, but due to the cyber attack the hospital was unable to perform the operation, and the patient died on the way to another hospital. German prosecutors pursued a murder charge against the hacker in the aftermath, but ultimately concluded that the charge could not be legally proven.

While there have likely been other deaths due to ransomware attacks on medical facilities, the direct connection here creates a new category of cyber risk.

Washington State Hacked

In December 2020, the state of Washington was hacked and more than 1.6M people may have had sensitive information exposed (names, bank account information, Social Security numbers

and more). The vulnerability appears to have been with Accellion, a third party vendor.

Vaccine Documents Unlawfully Accessed

The European Medicines Agency (EMA) confirmed that the regulatory submission for the BioNTech/Pfizer partnership for the Covid-19 vaccine was accessed during a hack on its server.

Pixlr Hack

Digital photography editing application, Pixlr has announced that 1.9M user records have been exposed.

Ransomware Attack on Environment Agency

Scottish Environment Protection Agency (SEPA) experienced a ransomware attack that affected the contact center, internal systems, processes and internal communication. Up to 4,000 files may have been stolen.

Hacker Attempts to Poison Water Supply

In another dangerous step into the world of physical harm from cyber breaches, a hacker was able to access the water control systems in Pinellas County, Florida and increased the level of sodium hydroxide to dangerous levels. The hack was accomplished through the remote access program intended for IT support, TeamViewer. Sodium hydroxide is used in small quantities to prevent pipe corrosion and increase pH but can be deadly in higher doses. The hacker changed the mix from 100ppm to 11,100ppm and a worker noticed the unusual activity and reversed the change immediately. Later evaluations found that the water control system had frighteningly little cyber security, used outdated software, shared passwords and had no firewall.

Big Tech

Instagram bug allowed app to turn camera on while app was closed

Amazon allegedly harvested and stored voice data in violation of BIPA

Twitter fined €450,000 under GDPR

Instagram sued and faces potential multibillion-dollar BIPA fine

Facebook, Twitter and Instagram fined $3.8M each for regulatory violations in Turkey

Australia continues to battle Google and Facebook over news rights

Regulatory and Legislative Update

OFAC Issues Guidance Update

In October 2020, the U.S. Department of the Treasury, Office of Foreign Assets Control (the entity that enforces sanctions violations) issued a guidance update that generated significant concern and commentary. The advisory itself doesn't alter existing regulations or rules but emphasizes how those regulations may apply in the context of ransomware payments and may signal renewed attention to the grey area surrounding ransom payments.

New York State Department of Financial Services (DFS) Initiates Enforcement Actions

In late July 2020, the New York State Department of Financial Services (responsible for enforcing New York's cybersecurity regulations) launched their first enforcement action. The action was against First American Title Insurance Company for alleged weaknesses in their systems that exposed 850M sensitive documents over the course of several years, including Social Security numbers, mortgage/tax records, bank accounts and more. The action remains pending but given the regulatory provision for $1,000 in fines per instance of private information being exposed, the civil penalty at stake is likely upwards of $1B.

DOJ Issues International Charges

In 2020, the U.S. Department of Justice (DOJ) charged a number of international hackers for cybercrimes. In September, the DOJ issued charges against Chinese and Malaysian hackers

for hacking and fraud in the video game industry. In October, they unsealed charges against six alleged Russian government hackers related to actions to the failure of Ukraine's power grid, interfering in French elections and other actions. Other charges were issued against Iranian hackers for intrusions, fraud, IP theft and more and against alleged Chinese State hackers for similar actions including additional IP theft.

New York Introduces Biometric Privacy Bill Mirroring Illinois' BIPA

The New York state legislature has proposed the Biometric Privacy Act to provide safeguards for consumers around the gathering and storage of biometric identifiers including fingerprints, voiceprints and facial recognition. If signed into law, the bill would put New York among a group of states with similar laws. The most notable aspect of the law is that it provides for a private right of action to pursue violations in civil court. The only other state to have such a provision is Illinois, and the impact there is still being measured.

Dating App To Be Fined

The Norwegian Data Protection Authority has issued a notice of intention to fine dating app Grindr NOK 100M under GDPR for disclosing personal data to third party advertisers without authority.

German Retailer Fined €10.4M for CCTV Monitoring of Employees

Computer retailer Notebooksbilliger used CCTV over a two year period to monitor employees and track the flow of goods in a warehouse and workspaces for the purpose of preventing theft. According to the State Commissioner for Data Protection (LfD) for the state of Lower Saxony, the tracking lacked legal basis as prescribed by GDPR.

EDPB Consults on GDPR Data Breach Notification Guidelines

The European Data Protection Board (EDPB) has begun a consultation period on its revised data breach notification guidelines. The guidelines are set to replace rules issued in October 2017. They are practice orientated and case based reflecting the experience of national supervising authorities since the implementation of GDPR. The scenarios include ransomware and exfiltration.

New EU Cybersecurity Strategy To Make Digital Critical Entities More Resilient

The European Commission has announced that it will reform rules under a directive on measures for high common levels of security across the Union, to improve the level of resilience of public and private sectors which include hospitals and energy grids.

Singapore Regulator Announces Amendments to Data Protection Act

The Personal Data Protection Commission (PDPC) of Singapore will phase in amendments to the Personal Data Protection Act (PDPA) which include mandatory data breach notifications, an expansion to the consent framework, increased financial penalties for organizations up to 10% of annual turnover or S$1M. Since its enactment in 2012, this is the first comprehensive review of PDPA. In November 2020, the amendments were passed and will be phased in starting February 2021.

Surge in Fines for Financial Institutions

Global data privacy for financial institutions reached $88.6M.

Interim Agreement on Personal Data Flow Post Brexit

Following Brexit, the treaty between the EU and the UK will allow data to flow freely pending a decision from the EU on the adequacy of the UK's data protection laws.

ICO Publishes Guidance on Using Algorithms for Employment Decisions

The UK regulator has highlighted six key points that organizations should consider when using algorithms to make hiring decisions. There is a concern that algorithms can worsen issues of fairness and inequality in an employment context.

Litigation News

Anthem Settles with State Attorneys General

In September 2020, Anthem settled the final open investigation around the 2016 cyber breach that affected nearly 79 million people. The settlement of $39.5M with the States is in addition to previous settlements of $16M with the DHS OCR and a $115M settlements of class action lawsuits arising from the breach, as well as the significant first part costs.

English High Court Tests Jurisdictional Reach of GDPR

The claimant, a UK resident and national, sought permission from the court to serve proceedings on defendants in the US. The complaint includes the misuse of private information focused on internet and social media posts that included photographs along with personal data that had been put into the public domain. Allegations included the misuse of cookies. GDPR enables proceedings to be brought in a member state where the claimant is resident. However, the court did not believe there was an arguable case under GDPR and considered the defendants use of the internet as a journalistic investigative tool.

CJEU Rules on Informed Consent

The Court of Justice of the European Union has ruled that a contract for providing telecommunications services that includes a clause stating that the data subject had been informed of, and has consented to, the collection and storage of a copy of his or her identity document for identification purposes did not demonstrate that the person had validly given his or her consent within the meaning of GDPR. The responsibility of demonstrating such consent was on the data controller.

U.S. 5th Circuit Court: Insurer Not on the Hook For BEC Claim

A US Court recently ruled that Axis Capital Holdings is not obligated to indemnify their insured after the insured wired over $1M to fraudsters who convinced them to change banking information for a known vendor via email. The policy at issue was a commercial crime policy, which had a $100K sublimit for social engineering fraud (which Axis paid). The policy also had a computer fraud cover with a $1M limit that was at issue in this case.

Cyber Publications

Beazley Breach Insights

Coveware's Q3 Ransomware Report and Q4 Ransomware Report

Allianz Cyber Risk Trends

Intel 471 - Ransomware as a Service

Veritas Ransomware Resiliency Report 2020

CrowdStrike's Global Security Attitude Survey

Gfeller Laurie – Vincent J. Vitkowsky – Cyber Risks and Insurance Coverage Decisions 2020

TransRe Speaks!

March 16th-19th Peter Cridland will join a panel to discuss cyber insurance issues at the International Bar Association's virtual Insurance Conference "Beyond Covid"

SPECIAL GUEST ARTICLE

Protecting Sensitive Forensic Reports: Applying Attorney-Client Privilege and the Work-Product Doctrine

By Al Saikali
Chair, Privacy and Data Security Practice
Shook, Hardy & Bacon, LLP

It is becoming increasingly the case that when a company suffers a data breach and makes the breach public, as it must where a breach notification law applies, the company is inevitably the target of a class action lawsuit. One of the first requests that a plaintiff's lawyer will make in such a lawsuit is for a copy of any report or analysis performed by the forensic cybersecurity firm, which investigated the incident. These reports are a gold mine for plaintiff's lawyers because they reveal the weaknesses in the breached company's cybersecurity system that led to the compromise, and help the plaintiff's lawyers establish theories of negligence and unfair trade practices for their lawsuit.

Until recently, the law on this issue was relatively friendly for companies that suffered data breaches. A company that performed a forensic investigation at the direction of counsel for the purpose of allowing counsel to provide legal advice to the company could not be forced to produce their forensic report in discovery. Such protection, however, is becoming less common. The most recent example of the eroding protection was an opinion issued by the U.S. District Court for the District of Columbia in a case called Wenguie v. Clark Hill. This article discusses the recent case, its implications, and how companies seeking to protect sensitive forensic reports can maximize the likelihood of such protection.

Background

The Wengui case arose from a cyberattack on a law firm (the defendant). The attackers allegedly obtained and then disseminated a former client's (the plaintiff's) confidential information on the Internet. The underlying allegations tell a dramatic story involving the plaintiff's escape from China. The plaintiff sought the defendant's representation in political asylum proceedings. The plaintiff warned the defendant that defendant's information security systems would be at risk if defendant accepted plaintiff's case. Sure enough, the defendant subsequently suffered a cyberattack, allegedly the result of a retaliatory act of state-sponsored cyber espionage that resulted in the theft of the plaintiff's personal information and subsequent dissemination of that information on the internet.

The defendant engaged outside litigation counsel to help prepare for litigation it anticipated from the attack. Outside litigation counsel, in turn, engaged a security-consulting firm to conduct a forensic investigation. It is not clear whether defendant's litigation counsel was also hired to provide legal advice regarding the defendant's rights and obligations under applicable data breach notification laws, data security laws, and contracts with third parties.

The Plaintiff's Requests

The plaintiff requested "all reports of [the defendant's] forensic investigation into the cyberattack." The defendant refused to provide the reports, asserting attorney-client privilege and the attorney work-product protection doctrine because the security firm was allegedly hired to assist outside litigation counsel "to prepare for litigation stemming from the attack."

In addition to requesting the forensic reports, the plaintiff served interrogatories seeking the defendant's understanding of why the attack occurred. The defendant refused to provide a response on the ground that "its 'understanding' of the progression of the incident is based solely on the advice of outside counsel and consultants retained by outside counsel" and therefore is privileged.

Lastly, the plaintiff sought "information or documents related to [the defendant's] clients other than Plaintiff" who may have been affected by the cyberattack. The defendant argued that this information was irrelevant and privileged.

What Did The Court Decide And Why?

The court rejected the defendant's attorney-client privilege and work product protection assertions. It allowed the plaintiff to obtain everything requested, including information about the defendant's other clients. Let's take each argument one at a time.

A. Work-Product Doctrine

Regarding the attorney work-product doctrine, the court ruled that the defendant failed to show that the forensic report wouldn't have otherwise

been created in the ordinary course of business irrespective of litigation. The court stated that it was "more likely than not, if not highly likely, that [the defendant] would have conducted an investigation into the attack's cause, nature, and effect irrespective of the prospect of litigation." The court noted that "substantially the same document would have been prepared in any event as part of the ordinary course of the defendant's business."

The defendant had argued that the forensic report was only one half of a two-tracked investigation: on one track, the defendant's usual cybersecurity vendor investigated and remediated the attack to preserve business continuity. The defendant did not assert privilege or work product over documents relating to that "ordinary-course investigation" work. On the second track, a forensic vendor was engaged by the defendant's outside counsel for the sole purpose of gathering information necessary for outside counsel to render legal advice. It was work product created in this second track that the defendant claimed was protected by the attorney work-product doctrine.

The court rejected the defendant's "two-track" argument. Essentially the court ruled that while defendant's argument would be correct in theory (i.e., if in fact the work had been performed as the defendant described) the work was not performed that way here. In reaching that conclusion the court cited:

- the lack of any sworn statement from the "ordinary course vendor" (the first track) supporting that the reason for its investigation was consistent with the defendant's assertion that it was performed for business continuity purposes;
- the defendant's own interrogatory response said that "its understanding of the progression of the [attack] is based solely on the advice of outside counsel and consultants retained by outside counsel" so how could that information have been the responsibility of the ordinary-course vendor;
- the ordinary-course vendor never produced any findings or a report like the one prepared by the forensic firm engaged by outside counsel;
- perhaps most significantly, the forensic firm's work picked up where the ordinary-course vendor's work ended, so the two were not in fact parallel tracks;
- the defendant's internal emails referred to the forensic firm engaged by outside counsel as "the incident response team";
- the forensic firm's report was shared with various members of the defendant's leadership, the defendant's IT team, and the FBI, not just in-house counsel, which demonstrated the purpose of the report was not for outside litigation counsel's purposes;
- the forensic firm's report was used to assist the defendant with management of "any" issues, "including" potential litigation; and,
- although the defendant "papered the arrangement using its attorneys," that approach appeared to have been designed to help shield material from disclosure.

It is possible that if only one or a few of these factors has existed, the result may have been different, but the fact that "the report was used for a range of non-litigation purposes" reinforced the court's determination that the document was not prepared in anticipation of litigation and therefore was not protected from discovery as attorney work-product.

B. Attorney-Client Privilege

Next, the court turned to the defendant's argument that the attorney-client privilege protected the forensic reports from discovery. Attorney-client privilege is intended to protect a confidential communication between attorney and client, where the communication is made for the purpose of obtaining or providing legal advice to a client. The privilege extends to reports of third parties made at the request of the attorney or the client where the purpose of the report was to put in usable form information obtained from the client. For example, a report by an accountant who makes a client's tax/financial information digestible for the attorney. However, where the advice sought is the accountant's rather than the lawyer's, no privilege exists.

Applying those principles here, the court held that the record showed defendant's true

objective was gleaning the forensic firm's expertise in cybersecurity, not obtaining legal advice from its outside counsel. The report provided detailed findings on how the defendant should tighten its cybersecurity, and the defendant shared the report with its IT staff and the FBI. Because the court decided privilege did not apply, it never reached the question of whether such privilege was waived when the defendant shared the report with the FBI.

The court ruled that the forensic report "and associated materials" were not privileged and needed to be disclosed, and the related interrogatories needed to be answered.

C. Information About The Defendant's Other Clients

Lastly, the court addressed the plaintiff's request for production seeking all documents reflecting that the attack resulted in a third party obtaining information, data, or material regarding any client of the defendant other than the plaintiff. The defendant objected to this request as irrelevant and privileged. The court nevertheless granted the plaintiff's motion to compel, ruling that the information was relevant to the central issue of the reasonableness of the defendant's cybersecurity, and that "appropriate redactions can assuage any privilege or privacy concerns" relating to other clients. This conclusion is somewhat concerning, since it could effectively require the defendant (a law firm) to provide the identity of its other clients to the plaintiff. But the court said that the law "does not protect from disclosure the identity of the client and the general purpose of the work performed" unless a client's identity is sufficiently intertwined with the client's confidences. The court suggested that the identity of the other clients could probably be redacted.

Where Does The Law Now Stand on Application of Privilege/ Work Product To Cybersecurity Information?

For a comprehensive analysis of the application of attorney-client privilege and the work product doctrine to cybersecurity information, I highly recommend that the reader dive into the fantastic commentary on that issue published by The Sedona Conference's Working Group on Privacy and Data Security Liability. It is, far and away, the best piece of legal writing on the subject, and a second edition may be in the works.

To be sure, there has been a trend with recent cases like *Wengui, In re Dominion Dental, and Capital One*, where courts are skeptical about the work-product doctrine and attorney-client privilege applying to forensic reports following a cybersecurity incident, let alone the application of those doctrines to proactive risk assessment reports where no cybersecurity incident has occurred. But the cases are mixed, and I believe that the outcome in any given case will be greatly impacted by the luck of the judge you draw and that judge's philosophy relating to the application of privilege and work product.

Nevertheless, to maximize the likelihood that the work-product doctrine or attorney-client privilege will apply to a forensic firm's report following a cybersecurity incident, the courts (and good cybersecurity counsel) will consider the following factors:

- How was the forensic vendor **engaged**? Through counsel or by the client? What was the scope of work envisioned in the vendor's statement of work? At whose direction was the forensic firm performing its work and for what purpose? How is the forensic vendor paid (by a company's business unit or their legal department)?

- What **protocols** were in place to protect confidentiality and ensure direct communication between counsel and the forensic firm? Was there a formal description of rules by which the client and forensic firm should abide to maintain confidentiality and privilege? Who had access to, and an ability to direct, the forensic firm?

- What procedures were in place with respect to **the forensic firm's deliverable**? To whom was it provided? How were drafts developed and reviewed? How and with whom was the report shared? How was it used to provide legal advice to the client?

- To what extent did counsel use a **shotgun approach to privilege or work product**, trying to apply the doctrines to engagements with

data restoration firms, mailing and call center services, and credit monitoring services? The overuse of the doctrines would create skepticism that it applied in the forensic context.

- The existence of a **parallel investigation** for business purposes, like the *Target* approach. This factor is tricky because companies cannot realistically be expected to afford the expense or the business interruption associated with a second, parallel investigation into the same incident. A better approach is reviewing the way in which the scope of the work was defined and performed (ensuring the work is more so for the purpose of giving legal advice rather than business/IT/InfoSec needs). At the very least, two reports (one for legal counsel and the other for the business) may be an option to consider.

These are high-level observations, and I implore readers to check out the Sedona commentary for a more fulsome analysis. Best of all, consult a lawyer who understands the legal and technical implications of these issues. In the meantime, it will be interesting to see over the next couple of years: will the application of privilege or work product to cybersecurity information remain, or will it be completely eviscerated?

Al Saikali chairs the Privacy and Data Security Practice for the law firm of Shook, Hardy & Bacon. He has been named by Chambers USA as a leading nationwide practitioner in privacy and data security law. Al and his team regularly represent companies in responding to cyberattacks and in class action lawsuit arising from cyberattacks.

IT Manager Article: The Pigeon and the Hawk

By Neil Inskip, SVP & IT Manager, TransRe London

As I write this article from my home study, I stare out of the window for a little inspiration and see a Sparrowhawk fly by carrying a pigeon (which is an amazing sight given the strength of the small bird and the pigeon being similar in size). I could continue to write about red kites that fly over or the muntjac deer that nibble my plants but it's probably not appropriate for this publication.

In this instance, I think we can all agree that there are enough criminals ready to predate our data or cash. I don't think it will come as a surprise that email attacks have increased during Covid-19 and email traffic has inevitably gone up. Employees are outside the protective bosom of their workplace and the demarcation that it provides. Some companies are less technologically advanced and did not think through their security strategy in time (or at all) for remote working.

So, as the pigeon, how do we react to the oncoming hawk? The game seems to have changed as we train our users to look for an external tag in the subject, spot poor spelling, check the actual SMTP email address (rather than trust the display name), look for urgency and tone in the content and if all else fails "trust your gut" and send it to the IT department for analysis. The email comes to guys like me to figure it out and we start the analysis by looking at the properties or email header, the bits you don't see unless you're looking. These show the message path, in terms of Internet address hops and other useful information (DKIM, SPF and DMARC checks). I won't get too technical but DKIM stands for DomainKeys Identified Mail which is an authentication method designed to detect when a sender email address has been forged (or spoofed as we call it). DKIM acts like a gatekeeper to validate the authenticity of email messages. Each company email server stores their unique electronic key which is used in the process to ensure the company is who they say they are. Sender Policy Framework (SPF) is a way that Internet service providers can verify that a mail server is authorized to send emails for a particular domain. It's essentially a whitelist of servers that are trustworthy to send emails on the domain owners behalf. Domain-based Message Authentication, Reporting & Conformance (DMARC) is an email authentication protocol that extends SPF and DKIM to add reporting capabilities and allow sender and receiver to improve and monitor protection of the domain from fraud emails.

One day I was forwarded an email for analysis so I checked the DMARC, DKIM and SPF and it all passed which makes you think that the company is good right? Well I still had a bad feeling since the body of the email contained only a link to a download site. The next step was to double check the senders Internet address. According to registration entries it belongs to the bona fide company too. Let's pause there, we could have paused and done the same thing right at the start, simply call the sender and ask if they sent anything. This is still an option for some emails, maybe broker/reinsurer relationships when the company is large with thousands of staff and you have no point of contact (that becomes tricky). I personally use a virtual sandbox where I test and send emails to see what happens (not connected to my network or the company). This last one was a credential harvester, you get a website screen that looks like Office365 (an exact replica) and if you provide your email and password expect it to be exposed.

In the end, the email came from an actual company, essentially a form of Business Email Compromise (BEC). The company most likely had their credentials stolen and the email was sent to contacts listed in their address book. To be frank, BEC is tough to deal with given it can feel 100% legitimate. In order to prepare, there are a lot of things you can do including training to improve the "gut instinct" and better anti-virus with some malware payloads. There are also contextual overlays you can put on email so your staff can get more information than just "External email exercise caution". These overlays can say if it's the first email you've received from the person, if the sender has a similar name to someone at your company and if the sender is dangerous etc. Again, it may not be too helpful for a cleverly crafted BEC. If you don't have an IT department to work with you could forward suspected emails to a third party for analysis as many security operations type companies now offer this service.

As I draw this article to a close, I look up again and see a relatively rare site in the UK, a black squirrel! Apparently imported in 1912 from the US to a private menagerie in my neighborhood. I'm happy this morning didn't go the other way around otherwise the bad guys would have been fluffy and hopping around burying their nuts!

TransRe™
cyber
We value risk.

New York

Underwriting

Alex Bustillo
T: 1 212 365 2376
E: abustillo@transre.com

Miguel Canals
T: 1 212 365 2266
E: mcanals@transre.com

Daniel Hojnowski
T: 1 212 365 2168
E: dhojnowski@transre.com

Actuarial

Joseph Marracello
T: 1 212 365 2159
E: jmarracello@transre.com

Claims

Peter Cridland
T: 1 212 365 2032
E: pcridland@transre.com

London

Underwriting

Rhett Hewitt
T: 44 (0)20 7204 8676
E: rhewitt@transre.com

Claims

Calum Kennedy
T: 44 (0)20 7204 8645
E: ckennedy@transre.com