Emerging trends in insurance coverage: Massive encryption attacks create urgent need for business interruption and cyber coverage

Received (in revised form): 12th December, 2017

Sean Hoar

CISSP, GISP, CIPP/US, has extensive experience managing responses to data breaches and working with cyber insurance carriers. As chair of the national Data Privacy and Cyber Security Practice at Lewis Brisbois Bisgaard & Smith LLP, he manages a national breach response team and personally manages responses to data breaches on a daily basis. He also counsels businesses on best practices in information privacy and data security. This includes incident response planning and employee/executive training on network security awareness. He served as the lead cyber attorney for the US Attorney's Office in Oregon, where he was the point of contact for the FBI, Secret Service and Homeland Security in system intrusions and other digital crime emergencies. He also taught courses in cybercrime and privacy law at the University of Oregon School of Law and the Lewis & Clark Law School, and he serves as executive director of the Financial Crimes & Digital Evidence Foundation. Sean holds the Certified Information Systems Security Professional (CISSP), the Global Information Security Professional (GISP) and the Certified Information Privacy Professional/United States (CIPP/US) credentials.

Lewis Brisbois Bisgaard & Smith LLP, 888 SW Fifth Avenue, Suite 900, Portland, OR 97204-2025, USA
Tel: +1 971-712-2795; E-mail: sean.hoar@lewisbrisbois.com

Peter M. Marchel

CPCU, ARM, RPLU, is president and founder of Marchel Risk Consulting LLC. Peter has extensive experience working with hundreds of insureds and insurance companies to draft and place management and professional liability policies, including cyber insurance policies. With more than 30 years' experience in legal and insurance matters, his background is unique — from working on insurance opinions as a former law clerk to Chief Justice Keith M. Callow of the Washington State Supreme Court, to arguing insurance cases before the court on behalf of both defendants and plaintiffs as a trial attorney. His experience as in-house Counsel and General Counsel for both insurance companies and insurance brokerages has brought a unique and valuable perspective to his clients. Peter consults with clients and their counsel on complex claims. He is a frequent speaker on Insurance and legal matters to local, regional and national organisations, including: ABA (American Bar Association); ACC (Association of Corporate Counsel); Washington State Bar Association; PLUS (Professional Liability Underwriting Society); CPCU (Chartered Property Casualty Underwriting Society); FEI (Financial Executive International); National Business Institute; Segal Graduate School of Business, Simon Fraser University, British Columbia, Canada; NACD (National Association of Corporate Directors); CBW (Community Bankers of Washington) and the Directors Roundtable. Peter serves as an expert witness for both defence and plaintiff firms in State and Federal Courts around the US, on insurance coverage, claims handling, bad-faith claims and agents and brokers professional liability matters.

Marchel Risk Consulting LLC, 12262 337th PL NE, Carnation, WA 98014, USA
Tel: +1 425-788-4349; E-mail: peterm@marchelassociates.com

Abstract The evolving online digital threats to businesses have created an urgent need for insurance coverage products to mitigate the risk of loss due to business interruption. This need is driven by the expanded digital environment in which our information resides. The amount of data generated, transmitted and stored by businesses continues to expand

at exponential rates. A related trend is that many businesses are going 'paperless', and an increasing number of professional services firms are storing all their data in the Cloud for enhanced security. Unfortunately, the more valuable the target, the more likely that it will be attacked. Consequently, malicious actors continue to follow the data into the cloud, which is not immune to data breaches. Businesses of all sizes, and in all sectors, continue to be targeted. If they have sensitive data (and most do), it can be stolen and monetised. If they have operational data (and all do), it can be encrypted and leveraged for extortion. If that were not enough, the cost of data security incidents continues to rise, in part due to increased regulation. All this is causing risk managers to pursue, with a sense of urgency, expanded business interruption and cyber insurance coverage to help mitigate both first and third-party economic risks. This paper reviews the trends in online digital threats, the corresponding trends in insurance coverage, and enterprise risk management measures that can be taken to better protect sensitive and operational data and mitigate the economic harm from data security incidents.

KEYWORDS: cyber security, data privacy, cyber insurance, risk mitigation, insurance coverage, business interruption

INTRODUCTION

The massive encryption attacks of 2017 have created an urgent need for insurance coverage products to mitigate the risk of loss due to business interruption. This need is driven by the expanded digital environment in which our information resides. The amount of data generated, transmitted and stored by businesses continues to expand at exponential rates.[1] A related trend is that many businesses are going 'paperless', and an increasing number of professional services firms are storing all their data in 'the cloud' for enhanced security.[2] Unfortunately, consistent with Sutton's Law,[3] the more profitable the target, the more likely it will be attacked. Consequently, malicious actors continue to follow the data into the cloud, which is not immune to data breaches.[4] Businesses of all sizes and in all sectors continue to be targeted — none are immune. If they have sensitive data (and most do), it can be stolen and monetised. If they have operational data (and all do), it can be encrypted and leveraged for extortion. If that were not enough, the cost of a data security incident continues to rise, in part due to increased regulation.[5] All this should cause risk managers to pursue, with a sense of urgency, expanded business interruption and cyber insurance coverage to help mitigate both first and third-party economic risks.

TRENDS IN MALICIOUS CYBERATTACKS

Until relatively recently, it may have been difficult to envision your network being rendered inaccessible or unresponsive. In 2012, the massive Saudi Aramco attack, in which over 35,000 computers were wiped or disabled within hours, provided some insight into the possible scale of devastation of a cyberattack.[6] The likely geopolitical reasons for the attack,[7] however, may have caused businesses outside the Middle East to see it as irrelevant to their digital security. Similarly, the 2014 massive hack on the Sony information system showed the devastating results of a malicious attack.[8] The possible political motivations behind the Sony attack,[9] however, may have caused businesses outside the entertainment sector to see it as irrelevant to their digital security. The massive encryption attacks of 2017,[10] however, may have been the wake-up call needed for

businesses of all sizes and in all sectors to see the weaponisation of encryption as a real threat to their networks.

Those of us who have responded to information security incidents (data breaches) on a daily basis over the years have witnessed a substantial evolution in the nature of the encryption attacks. A few years ago, encryption attacks typically took the form of a ransomware[11] attack in which malicious actors disseminated the malware randomly via phishing messages. When successful, their attacks often encrypted a relatively small 'network share'.[12] The ransomware message typically contained an attachment or a link. When the attachment was opened or the link clicked, the ransomware was executed on the device, its contents and the network share.

Many of the early ransomware attacks were not successful because the affected devices could be wiped or replaced, and the affected data could be replaced with data from backup systems. This may have caused businesses to see ransomware as more of an annoyance or inconvenience than a danger to their business model. Unfortunately, malicious actors learned from these experiences and now commonly corrupt backup systems and the backed-up data before launching the ransomware attack. This provides substantial leverage in a conventional ransomware attack, as the victim may have to consider paying a ransom depending upon the nature and value of the encrypted data. Due to the profitability of the criminal business models built around ransomware, it now has a pervasive presence within phishing messages.[13]

Ransomware attacks have also become increasingly sophisticated. Whereas they previously were disseminated randomly, they are now often committed through spear phishing.[14] The malicious actors conduct reconnaissance of an individual user and their information system, and craft an e-mail message with an attachment or link that the recipient is likely to open. The user is often someone that is likely to have access to valuable data, whether it be sensitive regulated data, operational data necessary for system functionality, or valuable proprietary data. When valuable encrypted data is combined with corrupted backups, it substantially increases the leverage of the malicious actor.

One of the challenges for information security personnel is that malicious actors are using encryption to carry out malicious attacks[15] — not simply to lock down devices or files, but as part of their entry into the systems. In a recent survey of over 1,000 information security professionals from various industries in North America and Europe, of 80 per cent of respondents who were victims of cyberattacks, 41 per cent of those attacks were hidden in Secure Sockets Layer (SSL) encrypted traffic to avoid detection.[16]

Another dangerous trend is that malicious actors are using encryption to not only carry out the attack, but to lock down evidence *after* a system has been compromised and sensitive data has been exfiltrated. Malicious actors have learned to use our familiarity with ransomware attacks to provide a ruse to cover their tracks after the severe compromise of systems. Businesses are increasingly experiencing what they believe to be a ransomware attack, due to the encryption of their devices and files, only to realise that it was not a ransomware attack but a full system compromise. In these attacks, malicious actors access a network, exfiltrate substantial amounts of sensitive data and then execute an encryption attack to lock down any forensic evidence that may have otherwise existed. The execution of the encryption attack may appear to be a ransomware attack, but increasingly it is being used as an anti-forensic measure to prevent investigators from acquiring the necessary evidence to attribute the attack to a specific malicious actor.

Unfortunately, the profitability of encryption attacks means they will only continue to occur, and will likely increase

in number and sophistication. Encryption attacks are a real threat to any business — and they can, and will, cause substantial interruption to businesses and their sources of revenue. It is therefore more important than ever for all businesses, regardless of size or sector, to take serious measures to not only secure their information systems, but to mitigate the economic risk of a catastrophic encryption attack. Whereas businesses in 2016 may have postponed the acquisition of business interruption insurance coverage to mitigate the economic impact of a cyberattack, businesses in 2018 should consider such coverage as a necessary component of enterprise risk management.

DETERMINING INSURANCE COVERAGE

Insurance coverage for cyber events continues to evolve. The insurance marketplace provides both standalone (monoline) cyber policies as well as cyber coverage 'add-ons' for different insurance policies. Cyber coverage add-ons can be found in policies such as professional liability, commercial liability, business owner's policy (BOP) and management liability.

Typically, add-on policies have low limits and do not provide the breadth or depth of coverage needed by most organisations. Cyber insurance coverage should be viewed as a policy providing 'access to resources' for a cyber event. The best way to obtain this coverage would be a standalone cyber policy. 'Access to resources' means an insurance policy which will provide: forensic services, both to determine the cause and extent of the cyber event; notification expenses, which may include credit monitoring and/or repair; legal assistance, which may include an assessment of consumer and regulatory notification obligations; crisis management (public relations); and assistance with regulatory investigations and enforcement actions.

It is important that organisations map their exposures and share their mapping with their insurance agent or broker. It is also imperative that organisations know their exposures and be proactive in asking about the types of coverage available and how the policy will respond to exposures of the organisation for specific cyber events.

Knowing your exposures

Mapping organisational cyber exposure is the process of identifying the type of data that exists within a network, determining its location and how it is secured, and learning about the relationship the data has to the business operations.

Knowing the type of data being processed, transmitted or stored and the number of data sets or records, is important to approximate the limits of cyber insurance that should be purchased. The type of data, whether it be protected health information (PHI), personally identifiable information (PII), payment card industry (PCI) data or other non-public data, including non-electronic data, will help to determine the value of the data and the expense of a potential data security incident. Knowing how the data is stored or protected is critical in determining the potential consumer and regulatory notification obligations.[17]

Knowing where and how the data is stored can also assist the forensics team to locate the cause and extent of the cyber event. This can reduce downtime as well as the expenses associated with the incident.

Knowing how the data is used in business operations can help an organisation determine the amount of first-party and business interruption coverage to be purchased. A good source of information to help determine what limits should be carried can be found in the NetDiligence 2016 Cyber Claims Study,[18] which provides information on claims service costs, cost per record and percentage of claims by data type. Another useful source of information

can be found at the Ponemon Institute.[19] This information can assist organisations in determining what limits should be considered for cyber coverages.

Coverages to look for within an insurance policy

There is no standard cyber insurance policy. Several insurance companies are now offering risk management services for policy holders, such as helplines, information portals and, in a few cases, preferred providers who can help insureds with pre-breach planning or other proactive avoidance at a reduced rate. Cyber policies can contain the following coverages:

First party
System damage
Business interruption
Reputational harm
Cybercrime
- Computer crime
- Identity theft
- Threats and extortion
- Telephone hacking
- Phishing scams

Regulatory actions and investigations
PCI fines and penalties

Third party
Cyber liability
Privacy liability
Notification costs
Multimedia liability and advertising injury

Organisations need to review their insurance policy carefully to determine if the above coverages exist in their policy. In addition, the policy should be reviewed to discern what limits are available for specific coverages within the policy, what if any sub-limits apply, and the applicable aggregate limit.

Cybercrime coverage

As discussed earlier, cybercrime is on the increase. The cyber policy should be reviewed to determine what coverages exist for cybercrime. One of the first steps organisations should take is to review what types of threat exist to their organisation. One of the best sources to obtain a greater understanding of the types of threat to your organisations is Verizon's Data Breach Digest[20] and Annual Data Breach Investigations Report.[21] The Verizon Data Breach Digest breaks cyber events into nine incident patterns: insider and privilege misuse, cyber-espionage, web application attacks, crimeware, point-of-sale intrusions, denial of service attacks, payment card skimmers, physical theft and loss, and miscellaneous errors. The same publication provides a heat map listing twelve victim industries and six different incident patterns.

We recommend that organisations review the narrative in each of the data breach scenarios in the Verizon Data Breach Digest to determine where possible cyber events could occur within their organisation. Similar to monitoring blood pressure, the data breach scenarios can alert an organisation to a possible exposure not previously considered.

Once threats have been identified, a thorough review of the cyber theft coverage should occur. Organisations should consider coverages for theft of data, theft of the economic value of intellectual property, theft of money or securities and theft of computing resources. Extortion and social engineering or deceptive funds transfer should also be evaluated. Organisations need to be proactive in knowing and understanding the types of exposure they face, so that they can ask their agent or broker how the policy will respond in a given cyber event. The cyber policy should be evaluated with the organisation's crime policy, if one exists, to determine any gaps or overlaps.

Business interruption coverage

Business interruption coverage is an exposure area that organisations must evaluate. The

cause of the disruption as well as the impact on the business need to be examined. Policy sub-limits, separate deductibles, wait periods and limited periods of indemnity for business interruption should all be reviewed carefully. Waiting periods can vary from eight to 24 hours or more.

A few policies will provide coverage for direct damage to equipment, and most policies will cover destruction of data either within the cyber policy or as an endorsement. Some policies will provide business interruption coverage, but only if it results from a security event and not for damage to physical hardware or equipment. A denial of services attack may also trigger a business interruption claim depending on the policy. Some policies may provide dependent business income loss coverage, which replaces loss of earnings because of a disruption sustained by a third party.

A cyber event can cause major disruption to an organisation, resulting in serious financial and reputational impact. A cyber business interruption claim can be more complex than other types of business interruption claims because of the less tangible nature of a cyber event and the potential reputational impact. The difference between cyber policy language for business interruption and reputational damages needs to be reviewed by organisations with care.

Regulatory fines, penalties and consumer redress funds

Organisations need to review their insurance policy to make sure that coverage for violation of regulatory acts, regulatory fines, penalties and consumer redress funds are available under the policy. Some policies will provide full limits for these areas of coverage, others will sub-limit the amount of coverage available. Most policies will exclude violations of various state, federal or foreign anti-spam or tele-marketing laws.

Another growing area of concern for organisations is alleged violations of the payment card industry (PCI) data security standard (DSS). Businesses that transmit PCI data typically have contractual obligations to merchant processors and card brands. In the event of a data security incident, these contractual obligations can result in large assessments for fraud monitoring, and large fines and penalties for fraud losses and card reissuance costs. Some policies provide coverage for this in their standard policy, while others may add this coverage by endorsement. Organisations should review their policy to determine if this coverage is available.

ENTERPRISE RISK MANAGEMENT

Insurance coverage

Appropriate insurance coverage should always be an aspect of enterprise risk management. In this evolving and increasingly dangerous digital environment, however, it can be overwhelming when considering other measures that must be taken to protect information systems. The following tips are not exhaustive, but will provide some guidance toward that end.

Regularly review security controls

In our own homes, we regularly check the locks to our doors when we leave for the day, or before we go to sleep at night. Similarly, we should regularly check the 'locks' to the doors on our networks. Whether it be confirming that the only devices accessing the network are those authorised to do so, or that the image loaded onto a laptop is the most secure version, every businesses should have a programme that involves the regular review of its security controls. As referenced below, while it is important to automate security checks when possible, it is important to periodically conduct a manual review of the network security controls to identify any gaps — which may include inadvertently

disabled automated controls. The review should begin with the foundational Critical Security Controls.[22]

Plan for data security incidents

Every business should have an incident response plan, regardless of its size or resources. Incident response plans should be mapped to the most recent version of the 'National Institute of Standards and Technology Computer Security Incident Handling Guide, Special Publication 800-61 (Rev. 2)'.[23] The planning process should include the identification and involvement of key stakeholders, the acquisition of cyber liability insurance, the facilitation and execution of Master Service Agreements with breach response service providers (digital forensics services, consumer notification/call centre services, credit monitoring/identity protection services, etc.) and introductions to appropriate law enforcement personnel. The incident response plan should also be tested on at least an annual basis. These tests are referred to as 'table top exercises'. These exercises should involve key stakeholders and assist them to identify and experience their roles and responsibilities in responding to a data security incident before an actual crisis occurs. 'Experiencing' a data security incident before it actually occurs accelerates an organisation's ability to effectively contain and remediate an incident. The exercises also help to identify and resolve gaps in incident response plans and enhance an organisation's enterprise security posture.

Automate security measures

As much as possible, security measures should be automated. Malicious actors will often utilise known vulnerabilities to access networks, and these known vulnerabilities often have available remediation measures. Whether it be security patches or threat detection software, the security measure should be automated when possible to minimise errors caused by human inaction.

Monitor and review third-party liability

The Target cyberattack was a wake-up call regarding third parties being used as attack vectors.[24] We now know that third-party liability must be managed as closely as any other information security control. This can be accomplished in part through narrowly tailored service provider agreements designed to mitigate potential exposure arising from a data security incident. These agreements should require the service provider to adhere to delineated information security practices moulded to the specific service offering. The agreements should also set forth expectations as to when, how and under what circumstances a service provider must report a potential or suspected data security incident. They should also preserve the business's right to conduct an independent forensic investigation and consider incorporation of indemnification and limitation of liability language to shift liability and defence exposure to the service provider. They should also require the service provider to carry sufficient insurance coverage to mitigate the economic risk they might pose to the business as an attack vector. With the evolution of technology and online threats creating an increasingly dangerous digital environment, managing liabilities associated with service providers has never been more important. The risks and liabilities can be mitigated, however, with due diligence and good service provider contract management.

Whitelist apps

Third-party apps are increasingly integrated into virtual networks, but are often not very secure. It is important to identify the apps that are being used for legitimate business purposes, and to authorise or 'whitelist' only those apps for use on our networks. It is very important to ensure that the authorised

apps are the latest, most secure versions, and that any necessary security patches be immediately installed.

Delete unnecessary data

Much like sensitive data in non-digital form which should be shredded when it is no longer necessary for legitimate business purposes, once sensitive data in digital form is no longer necessary for legitimate business purposes, it should be deleted. The prompt deletion of unnecessary data decreases potential liability for the business in the event of a data breach.

Minimise downloads

The less a business downloads sensitive data, the better. The goal is to have the fewest sensitive data sets in in-house systems, and one way to accomplish this is to reduce the number of downloads — whether they be from insecure Internet sites or from secure storage areas. The fewer sensitive data sets that might be available to a malicious actor, the less potential liability for the business in the event of a data breach.

Embrace tokenisation

Tokenisation is a method for protecting sensitive data and is commonly used with point-of-sale systems to protect payment card data. It can protect other types of sensitive data as well, and should be considered when appropriate. Tokenisation associates data with a temporary random alternative — the token — typically used to transfer the data. The token then replaces the data during the transfer. If the transferring network were to be compromised, the data would be useless to a malicious actor.

CONCLUSION

The massive encryption attacks of 2017 should be a clarion call for insurance coverage products to mitigate the risk of loss due to business interruption. As businesses continue to process and store more valuable data, they will increasingly be targeted by malicious actors who seek to monetise the data. The more profitable the target, the more likely it will be attacked. As discussed above, if businesses have sensitive data (and most do), it can be stolen and monetised. If they have operational data (and all do), it can be encrypted and leveraged for extortion. All this should cause risk managers to pursue, with a sense of urgency, expanded business interruption and cyber insurance coverage to help mitigate the potential — and very real — economic risks posed by malicious encryption attacks.

References

1. The size of the digital universe is expected to continue to double every two years, a 50-fold growth from 2010 to 2020. See 'The Exponential Growth of Data', available at https://insidebigdata.com/2017/02/16/the-exponential-growth-of-data/ (accessed 27th July, 2018).
2. Multiple sources predict a continued and substantial increase in spending on cloud computing. See 'Roundup of Cloud Computing Forecasts, 2017', available at https://www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts-2017/#13263bc831e8 (accessed 27th July, 2018).
3. *New York Herald* reporter Mitch Ohnstad wrote that when Willie Sutton was asked why he robbed banks, he replied 'Because that's where the money is'. This evolved into 'Sutton's Law' as a metaphor for focusing on the most likely result of one's efforts, or the most likely conclusion from the evidence.
4. See '7 Most Infamous Cloud Security Breaches', available at https://www.storagecraft.com/blog/7-infamous-cloud-security-breaches/ (accessed 27th July, 2018).
5. See 'Global Cyber Market Review', available at http://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf (accessed 27th July, 2018).
6. See CNN, 'The inside story of the biggest hack in history', available at http://money.cnn.com/2015/08/05/technology/aramco-hack/index.html (accessed 27th July, 2018).
7. See 'Hackers Lay Claim to Saudi Aramco Attack', available at https://mobile.nytimes.com/blogs/bits/2012/08/23/hackers-lay-claim-to-saudi-aramco-cyberattack/ (accessed 27th July, 2018).
8. See 'The Sony Pictures hack, explained', available at https://www.washingtonpost.com/news/

the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.cd17792852fd (accessed 27th July, 2018).

9. See 'U.S. Said to Find North Korea Ordered Cyber Attack on Sony', available at https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html (accessed 27th July, 2018).
10. See 'Ransomware and Encryption Attacks', available at http://lewisbrisbois.com/practices/data-privacy-cyber-security/blog/ransomware-and-encryption-attacks (accessed 27th July, 2018).
11. See 'Ransomware: The Tool of Choice for Cyber Extortion', available at https://www.fireeye.com/current-threats/what-is-cyber-security/ransomware.html (accessed 27th July, 2018).
12. The network share is comprised of all those devices connected on a network that can be accessed by the users. This means that if a device is connected to a server and a printer, the network share is at least comprised of those devices. See definition of 'network share', available at https://www.pcmag.com/encyclopedia/term/47915/network-share (accessed 27th July, 2018).
13. See '93% of phishing emails are now ransomware', available at https://www.csoonline.com/article/3077434/security/93-of-phishing-emails-are-now-ransomware.html (accessed 27th July, 2018).
14. Spear phishing is typically conducted via e-mail that is targeted toward a specific individual — although it can also encompass an organization or business. See Google search, available at https://www.google.com/search?q=spear+phishing+def&oq=spear+phishing+def&aqs=chrome..69i57j69i61j69i60l2.8201j0j4&sourceid=chrome&ie=UTF-8 (accessed 27th July, 2018).
15. See Sonic Wall (July 2017), 'State of Encrypted Traffic — New Cyber Attacks Spreading via Use of Encryption', available at https://blog.sonicwall.com/2017/07/state-of-encrypted-traffic-new-cyber-attacks-spreading-via-use-of-encryption/ (accessed 27th July, 2018).
16. *Ibid*., note 15.
17. Forty-nine of the state data breach notification statutes include a safe harbor for encrypted personal information. See http://lewisbrisbois.com/privacy/US (accessed 27th July, 2018).
18. NetDiligence 2017 Cyber Claims Study, available at (accessed).
19. Ponemon, available at https://www.ponemon.org/library (accessed 27th July, 2018).
20. Verizon, 'Date Breach Digest', available at http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017/ (accessed 27th July, 2018).
21. Verizon, 'Tales of Dirty Deeds and Unscrupulous Activitoes', available at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/ (accessed 27th July, 2018).
22. The Critical Security Controls are a recommended set of actions for information security. They are recognised as providing specific actionable measures to defend against pervasive and dangerous attacks. They also prioritise measures to be take which will provide the best results. See Sand, available at https://www.sans.org/critical-security-controls (accessed 27th July, 2018).
23. See 'Computer Security Incident Handling Guide', available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (accessed 27th July, 2018).
24. See 'Case Study: Critical Security Controls that Could Have Prevented Target Breach', available at https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412 (accessed 27th July, 2018).