Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

researchers in a number of disciplines and in a fast-changing landscape.

References

1. Paganini, Pierluigi. 'Spear-phishing attacks hit the oil and gas industry sector'. Security Affairs, 21 Apr 2020. Accessed Oct 2020. https://securityaffairs.co/wordpress/101967/cybercrime/spear-phishing-energy-oil-gas-industry.html.
2. Park, Donghui; Summers, Julia; Walstrom, Michael. 'Cyber attack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks'. University of Washington, 11 Oct 2017. Accessed Oct 2020. https://jsis.washington.edu/news/cyber attack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

How organisations can ethically negotiate ransomware payments

Tom Hofmann

Tom Hofmann, Flashpoint

By 2021, a new organisation will be falling victim to ransomware every 11 seconds.[1] However, ransomware figures have been skyrocketing since 2017 when the globe was hit by WannaCry and NotPetya. At that time, the term 'ransomware' entered common parlance and 54% of businesses were hit by these attacks.

These numbers are even more striking when considering the average cost of a single ransomware attack. Before even paying the ransom, the accumulated cost of downtime, people time, device cost, network cost and lost opportunity is estimated to be around $713,000 on average.[2]

So, how do the majority of businesses that are targeted by these insidious attacks deal with them? While it is an IT or IT security responsibility to protect and remediate against ransomware, the onus lies on business leaders to make the ultimate decision – to pay or not to pay. And for many this raises an ethical dilemma.

Many leaders will initially take the higher ground because they don't want to be seen as a business that negotiates with criminals or sends money to people who may invest it into other illicit activities such as drug or weapons dealing. On the flip side, depending on what is being held to ransom, whether that is personal data that it is an organisation's role to protect, critical infrastructure or even life-saving medical devices, sometimes organisations have no option but to pay. And with 95% of organisations that pay the ransom having their data or systems restored to them, for many this is simply the safer strategy.

This article will discuss the latest ransomware trends before giving some insight into unspoken codes of conduct among cyber criminal groups that will help readers understand the inner workings of why these attacks happen. It will then conclude with some advice on how to negotiate with cyber criminals to lessen the impact on the organisation, if this is a safer and more ethical option for businesses than not paying.

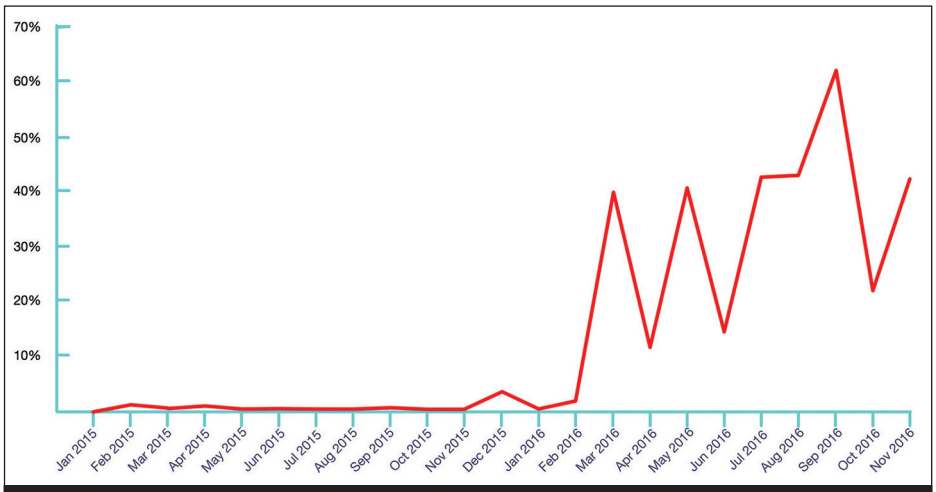
Ultimately, paying the ransom should always be the last option, but if a business has no other choice, ensuring that the payment and remediation process is completed strategically and in a safe manner is paramount to the business recovering as quickly as possible.

Latest trends

The 2016 ransomware attack against the Hollywood Presbyterian Medical Centre was a turning point in the history of ransomware.[3] It was the first attack that put human lives at risk (threatening to turn off life-saving equipment) and – even though the hospital claimed the infrastructure was never truly at risk – Hollywood Presbyterian paid the 40 bitcoin ransom ($17,000 in 2016 but worth over $400,000 today) in just over a week. In the following months, ransomware globally increased by 6,000% and 70% of businesses affected chose to pay the ransom.[4]

Over the following year, the world was rocked by the likes of WannaCry, NotPetya and CryptoLocker, which are still widely considered the largest ransomware attacks to have ever taken place. However, since then this indiscriminate attack style has been replaced by a more targeted approach, run by more nimble threat actors.[5]

While still largely relying on commodity exploits for known vulnerabilities or configuration weaknesses to gain access to a network, rather than dropping malware on certain machines, attackers have been hitting organisations hard by flooding ransomware onto endpoints and network shares and demanding drastically high ransoms in return for decrypted data. Already, state and local government operations have suffered major incursions, with one of the biggest being the attack against the city of Atlanta in 2018. Atlanta was infected, according to investigators, with the SamSam ransomware, which is spread via exploits rather than through shotgun-style spam or phishing emails.[6] Victims in other industries, notably financial

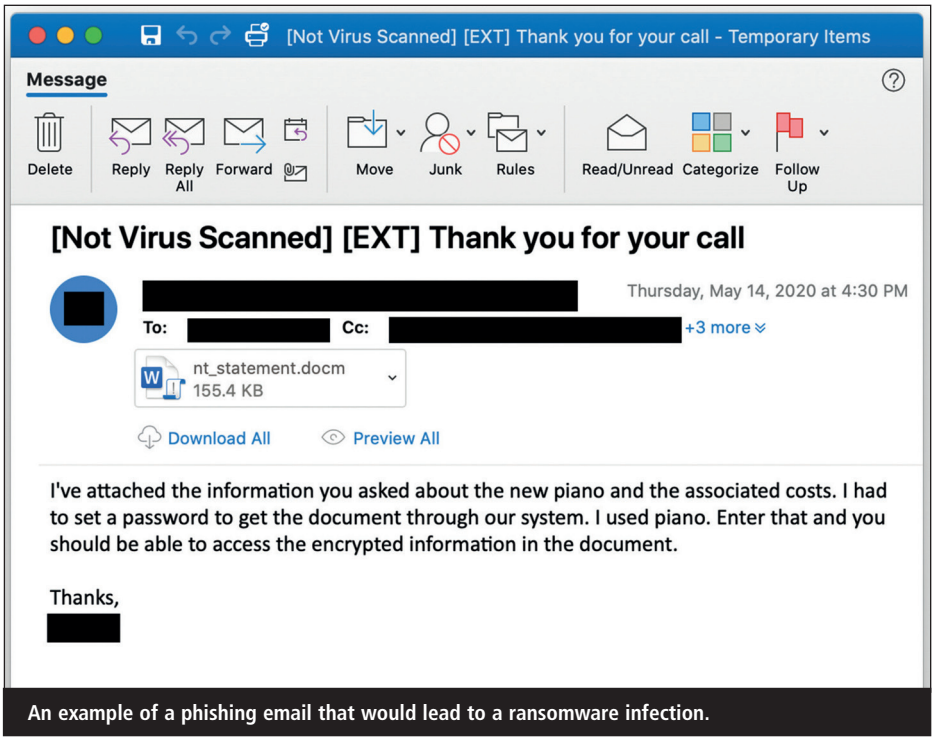


Percentage of spam with ransomware attachments, showing how the ransomware menace fully emerged in 2016. Source: IBM.

services, telecommunications and healthcare, have also felt the brunt of targeted ransomware attacks.

This section will conclude with three of the most recent ransomware trends. First, ransomware-as-a-service – these programmes have been developed with great care to ensure that encrypted files can be successfully restored after the ransom is paid in order to keep these attacks as a viable way of making money. Second, ransomware attacks are increasingly focused on threatening to leak data if the ransom isn't paid, with leak sites including AKO, CLOP and DoppelPaymer.[7] This trend reflects the development of global data protection regulations such as the General Data Protection Regulation (GDPR) which have significant financial repercussions for organisations experiencing breaches, leading to a higher probability of firms paying the ransom to prevent breaches altogether.

Finally, the coronavirus pandemic has seen an explosion of themed attacks of all varieties. Ransomware has been less common than phishing and fraud-related attacks but we have seen some groups targeting healthcare organisations. For example, the Maze ransomware group conducted an attack on Hammersmith Medicines Research, which performs clinical tests for drugs and vaccines.[8]



An example of a phishing email that would lead to a ransomware infection.

Codes of conduct

While the latest ransomware trends are frequently discussed in cyber security forums and recently in more mainstream media as well, cyber criminal communications about ransomware and the nuances of their activities are shadier. Readers may be surprised to learn that despite the popular image of the hooded, faceless cyber criminal, generating a notion that these individuals are less than human, there is in fact an unspoken code of conduct within cyber criminal communities and these attacks can cause 'ethical dilemmas' for hackers perpetrating ransomware attacks.

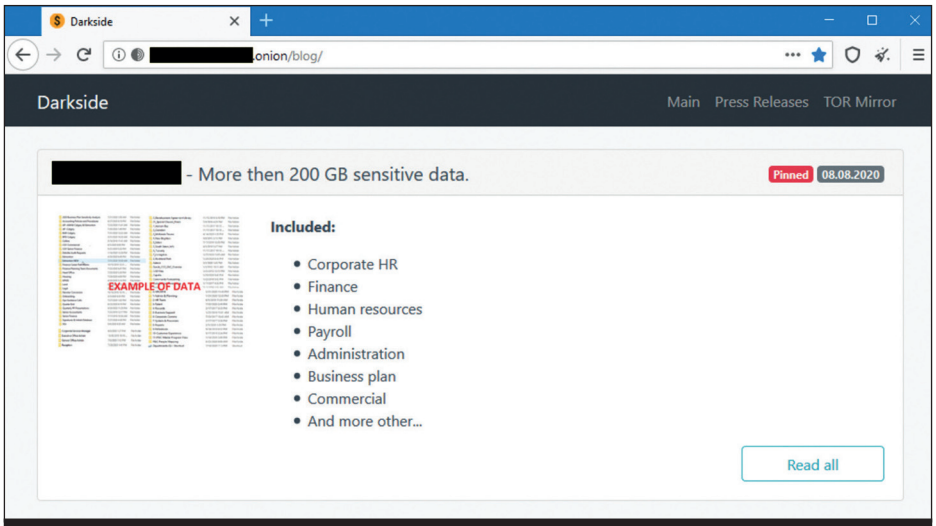
For example, while monitoring online illicit communities in Eastern Europe from early 2014 to early 2016, Flashpoint identified the forewarnings of a shift in attitude towards ransomware.[9] Prior to 2016, administrators of the Russian cybercrime underground stated that ransomware should not be practised for two reasons: either it was a waste of botnet installs and exploit kits or it was seen as 'intellectual death' and therefore a low-end manoeuvre.

These administrators firmly believed that ransomware attracts too much attention, may impede other types of cybercrime or could be too easily turned toward Russian targets. The increase may cause the Russian Government to take a harsher stance towards deep and dark web communities.

Cold reception

Returning back to Hollywood Presbyterian, despite this attack targeting Westerners – which is highly encouraged by many cyber criminal groups – it was coldly received by Eastern European cyber criminals, many of whom regarded the incident as reckless and unacceptable. While some in the community supported the attack, the majority condemned the unknown assailants, which created an ethical divide in the underground.

One highly reputable member of a Russian top-tier cybercrime forum expressed his frustration with ransomware, writing: "From the bottom of my heart, I sincerely wish that the mothers of all ransomware distributors end up in the hos-



An example of a data leak page from a ransomware group – in this case, Darkside.

pital, and that the computer responsible for the resuscitation machine gets infected with [the ransomware].” In response, a prominent ransomware operator countered that view: “[the attackers] scored. It means everything was done properly.” Rather than adhering to the ethical code imposed by administrators, he proposed that targeting places that were guaranteed to pay was not wrong because, at the end of the day, cybercrime is always about making money.

Unfortunately, this latter way of thinking appeared to win the debate, as from 2016 (WannaCry debilitating the NHS as a case and point) criminal perceptions of ransomware appeared to move beyond ethical concerns into being largely financially motivated. The majority of those perpetrating these kinds of attacks do, however, encourage each other to live up to the promises they gave to their victims, otherwise ransomware could lose its money-making power (this is echoed in the statistic at the top of this article, that 95% of people who have paid a ransom had their data restored to them).

The purpose of this section has been to showcase that when defending the organisation against any cyber security threat, seeing cyber criminals as people rather than shadowy figures without nuanced motivations or ethics is key in protecting organisations from attack. The combination of monitoring activity in the deep and dark web and closely monitoring observed attacker behaviours inside the organisational environment yields a much deeper perspective on the actors threatening the business. This dramatically improves situational awareness and provides necessary perspective when developing effective mitigation strategies for defence.

When to negotiate

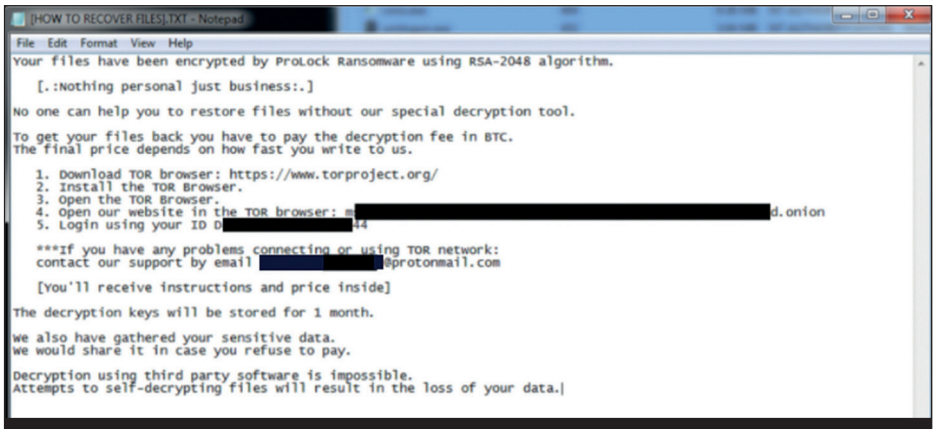
On 7 May 2019, the City of Baltimore in Maryland was hit by a ransomware attack.[10] The attack shut down the majority of the city’s servers, meaning online services and more were completely shut down while the attackers demanded a 13 bitcoin ($100,000) ransom. But Baltimore never conceded. Instead it focused all of its efforts on forensic analysis and detection, deploying new systems, hardware and software, replacing hard drives and additional recovery at a cost of $18.2m.

Baltimore was able to recover without paying the ransom but organisations must understand that paying a ransom can drift toward becoming a viable option when weighed against unacceptable losses that system and service unavailability may bring to an enterprise or government or civilian agency. This flies in the face of stern recommendations from law enforcement and the security community, both of which are adamant against paying for fear of propping up a criminal ecosystem, and without a steadfast guarantee that encrypted files and locked-down systems will be returned intact.

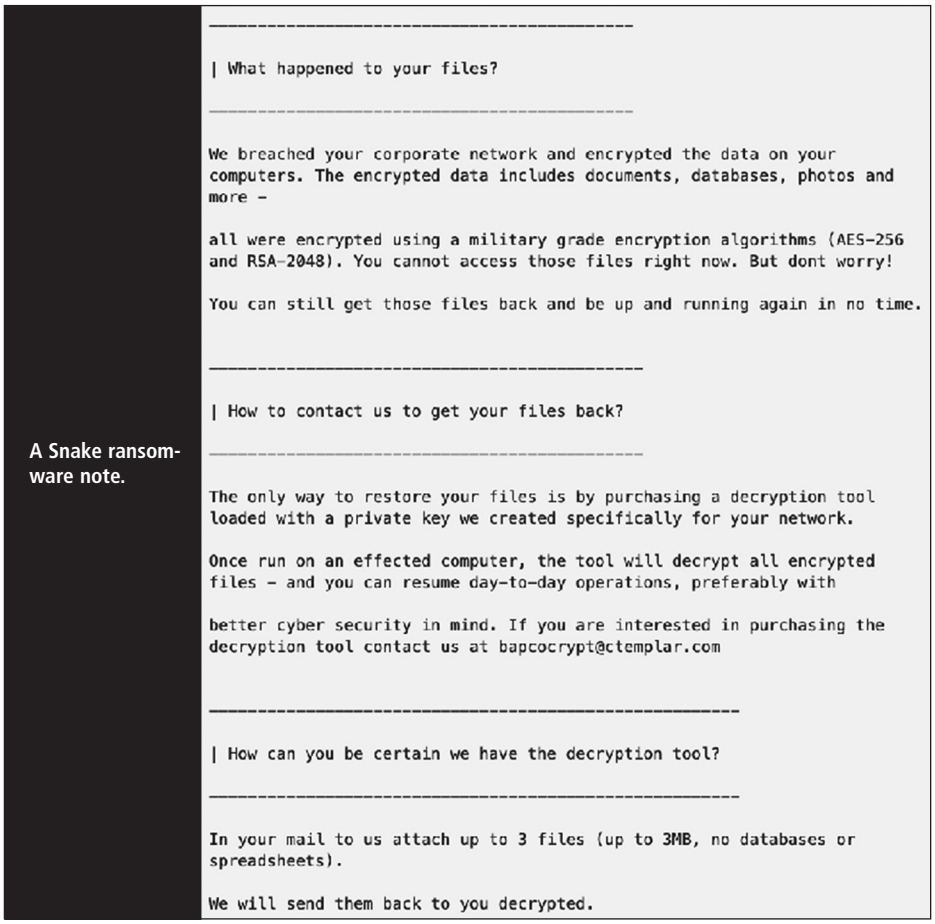
The immediate and future financial viability of a company and fiduciary responsibility to stakeholders could heavily sway such a conversation toward meeting an attacker’s demands. Even so, organisations must tread carefully should they choose to pay; there are no guarantees that a decryption key will be delivered, nor would there be an assurance that files haven’t been corrupted, or that internal staff have the wherewithal to handle the keys properly and decrypt every file and unlock every system.

Nonetheless, research and advisory firm Forrester Research also says it has been tracking a notable increase in ransomware payouts.[11] Its analysts now recommend that paying ransomware should at least be considered a viable option in order to offset potentially catastrophic business interruption. The firm does remind potential victims that paying a ransom isn’t an automatic path to recovery, which is complicated in any extortion scam.

The long and short of this is that organisations should always be prepared to be targeted by a ransomware attack: and with this in mind, back-up is a victim’s best friend. A recent, reliable and secure back-up can have an organisation



A Prolock ransomware note requesting an amount in Bitcoin that “depends on how fast you write to us”.



```
------------------------------------------

| What happened to your files?

------------------------------------------

We breached your corporate network and encrypted the data on your
computers. The encrypted data includes documents, databases, photos and
more -

all were encrypted using a military grade encryption algorithms (AES-256
and RSA-2048). You cannot access those files right now. But dont worry!

You can still get those files back and be up and running again in no time.


------------------------------------------

| How to contact us to get your files back?

------------------------------------------

The only way to restore your files is by purchasing a decryption tool
loaded with a private key we created specifically for your network.

Once run on an effected computer, the tool will decrypt all encrypted
files - and you can resume day-to-day operations, preferably with

better cyber security in mind. If you are interested in purchasing the
decryption tool contact us at bapcocrypt@ctemplar.com


------------------------------------------------------

| How can you be certain we have the decryption tool?

------------------------------------------------------

In your mail to us attach up to 3 files (up to 3MB, no databases or
spreadsheets).

We will send them back to you decrypted.
```

A Snake ransomware note.

up and running relatively quickly and with minimal downtime. It will also be spared the potentially risky task of engaging directly with a threat actor, as well as procuring and transferring crypto-currency to meet the attacker's ransom demand. These tasks aren't covered in traditional incident response plans where system clean-up and reimaging is self-contained and can be accomplished in relatively short order.

However, if restoring a back-up isn't an option because it will take too long or there are other ethical barriers in place – for example, if critical technology has been shut down – firms may have to turn to incident response and, potentially, ransomware negotiation.

Effective bargaining

As this article has argued, the driving factors behind whether to pay a ransom or not are twofold: ethical (if what is at stake is very sensitive personal data, critical infrastructure or people's lives) and financial (if the cost of downtime will exceed the cost of the ransom). So, if an organisation decides to pay the ransom, what actions must it take to ensure that the process is handled as professionally and safely as possible?

First, conventional incident response must take place, where the team runs forensics and validates the possibility of recovering data and systems from back-up. In parallel with this, firms must begin communication with the attacker, which could include negotiation for a discount and validation by asking for a decrypted key. It is highly recommended that you use a negotiation specialist for this because he or she will bring expertise in particular ransomware strains as well as re the threat actors. That type of intelligence can help an organisation make its final decision and understand whether successful recovery is possible. There's also a skill to the negotiation and professionalism provided by someone marginally detached from the incident.

Key elements of the negotiation process include demanding a 'proof of life' from the hackers, whereby the business requests they decrypt a portion of the hostage files. Organisations must also try their utmost to pay out strategically – they must work quickly to identify which critical operations need to be restored urgently and which could be rebuilt at less cost than paying the ransom. They can then negotiate an immediate payment with the criminal to restore these systems before quickly backing them up so they are fortified against being attacked again.

Ever-changing threats

To conclude, this article has tracked the evolution of ransomware from when it became one of the most used forms of cyber attack in 2016, examining the different forms it has taken today to showcase how it is always evolving. For this reason, all organisations should maintain an ongoing interest in protecting themselves from the ever-changing threats and attack methods used. It then examined the changing ethics of threat actors to highlight the importance of seeing cyber criminals as human beings with a host of different motivations. As a result, having a team or partner that understands threat actors can make a huge difference in defending against and responding quickly to not just ransomware but all kinds of cyber attacks.

We concluded with an analysis of the 'to pay or not to pay' alongside actionable advice on incident response and ransomware negotiation. As argued throughout, decision-makers must make the call as to whether to pay in a ransomware incident, and only after all options have been considered and all recovery options exhausted. Ultimately, paying a ransom demand is a business decision and one that organisations must prepare for in advance by contracting with a negotiations specialist and consider procuring crypto-currency in the event of an infection.

Often, specific expertise isn't in the wheelhouse of an enterprise's incident response team; ransomware requires a new paradigm of contingencies related to response. Few organisations today know how to best interact with an adversary, acquire crypto-currency and successfully and safely move that money to an attacker's wallet without putting the firm at further risk. When it comes to ransomware, the popular phrase "it's not a matter of if it will happen to you, but when" applies.

Being as prepared as possible to respond to an attack is business critical.

About the author

Tom Hofmann leads the intelligence directorate at Flashpoint that is responsible for the collection, analysis, production and dissemination of deep and dark web data. He works closely with clients to prioritise their intelligence requirements and ensures that internal Flashpoint operations are aligned to those needs. Hofmann has been at the forefront of cyber intelligence operations in the commercial, government and military sectors, and is known for his ability to drive effective intelligence operations to support offensive and defensive network operations.

References

1. Morgan, Steve. '2017 Cybercrime Report'. Cyber security Ventures, Feb 2017. Accessed Aug 2020. https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf.
2. Graham, Luke. 'Ransomware can cost firms over $700,000; cloud computing may provide the protection they need.' CNBC, Aug 2020. Accessed Aug 2020. www.cnbc.com/2017/08/04/cloud-computing-cyber security-defend-against-ransomware-hacks.html.
3. Yadron, Danny. 'Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers'. The Guardian, Feb 2016. Accessed Jul 2020. www.theguardian.com/technology/2016/feb/17/los-angeles-hospital-hacked-ransom-bitcoin-hollywood-presbyterian-medical-centre.
4. 'Ransomware: How consumers and businesses value their data.' IBM, Dec 2016. Accessed Jul 2020. www.ibm.com/account/reg/us-en/signup?formid=mrs-form-10908.
5. 'The crippling effects of targeted ransomware attacks.' Flashpoint, Apr 2016. Accessed Jul 2020. www.flashpoint-intel.com/blog/cybercrime/the-crippling-effects-of-targeted-ransomware-attacks/.
6. Ventura, Vitor. 'SamSam – The Evolution continues netting over $325,000 in 4 weeks'. Talos Blog, 22 Jan 2018. Accessed Jul 2020. https://blog.talosintelligence.com/2018/01/samsam-evolution-continues-netting-over.html.
7. Cimpanu, Catalin. 'Here's a list of all the ransomware gangs who will steal and leak your data if you don't pay.' ZD NET, Apr 2020. Accessed Aug 2020. www.zdnet.com/article/heres-a-list-of-all-the-ransomware-gangs-who-will-steal-and-leak-your-data-if-you-dont-pay/.
8. 'HMR targeted by cyber criminals'. Hammersmith Medicines Research, 29 Apr 2020. Accessed Jul 2020. www.hmrlondon.com/hmr-targeted-by-cyber criminals.
9. 'How ransomware has become an 'ethical' dilemma in the Eastern European underground'. Flashpoint, 20 Sep 2017. Accessed Jul 2020. www.flashpoint-intel.com/blog/ransomware-ethical-dilemma-eastern-european-underground/.
10. 'Here's what went wrong in the Baltimore ransomware attack that cost the city $18.2 million' Cyware Social, 1 Oct 2019. Accessed Jul 2020. https://cyware.com/news/heres-what-went-wrong-in-baltimore-ransomware-attack-that-cost-the-city-over-182-million-3b6ac1a2.
11. Zelonis, Josh; Lyness, Trevor; Balaouras, Stephanie; Cyr, Madeline; Dostie, Peggy. 'Forrester's guide to paying ransomware: paying ransom can be a valid recovery option based on business need and circumstances'. Forrester, Jun 2019. Accessed Jul 2020. www.forrester.com/report/Forresters+Guide+To+Paying+Ransomware/-/E-RES154595.

Data highway and the digital transformation: arguments for secure, centralised log management

Robert Meyers

Robert Meyers, One Identity

Digital transformation happened all of a sudden, not with a gradual shift towards more sophisticated tools, but with a televised announcement from prime ministers and presidents across the globe asking organisations to do their part in containing the coronavirus outbreak. Almost overnight, companies found themselves having to adapt to a completely new mode of working. Some saw their remote workforce increasing exponentially, others had to swiftly make arrangements as they had previously always worked on-premise.

Faced with this challenge, companies had to put policies and technologies in place to allow employees to continue doing their job as they would have in the office. That meant that all the tools workers