White Paper

HardenStance

Adjusting to a New Era in Ransomware Risk

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

April 2022

Executive Summary

- Changes in ransomware business models, new government interventions in the market, and more expensive cyber insurance premiums, should drive an urgent review of cyber risk exposure and cyber security posture relative to ransomware.
- There had already been a steep increase in ransomware risk leading up to February 24th, 2022. Russia's fateful invasion of Ukraine has ratcheted up the risk still further.
- This new era in ransomware risk points to a need for organizations to prioritize reviewing ransom payment policies; cyber attack response plans; cyber insurance policies; operational security with MSP partners; and RDP security policies.

Russia's invasion of Ukraine has introduced a lot more uncertainty into the discipline of ransomware risk assessment and risk mitigation.

Russia's Invasion of Ukraine Creates New Risk

In the months leading up to February 24th, 2022, many organizations were already struggling to understand the implications of a host of new changes in the ransomware landscape that began emerging during 2021. Russia's invasion of Ukraine that day, and the resulting imposition of severe sanctions on Russia's economy, has introduced even more uncertainty into ransomware risk assessment and risk mitigation.

This White Paper assesses ransomware risk in 2022 in light of a transformation in the market-leading up to the start of Russia's war and the additional uncertainties now arising from it. It lays out the potential opportunities and threats that both the war and global economic sanctions create for ransomware gangs around the world, notably those based in Russia itself that are responsible for the majority of ransomware attacks.

It describes the marked escalation in different government interventions in the workings of the ransomware ecosystem during the second half of 2021 and considers what direction government intervention may now take not just in relation to ransomware gangs but into how businesses respond to ransomware attacks. This White Paper also assesses the aggregate impact of these changes on ransomware risk and prescribes mitigation steps that organizations should be prioritizing in light of these changes.

Ransomware has been around for many years. Until recently, it was more of a nuisance and a financial cost that only affected victim organizations themselves. It typically affected individual machines and the ransom payments were relatively small. Ransomware continued evolving in 2018-2019 but, as discussed on page 4, it's really in the last two years that it has been transformed by the force multiplier of Ransomware as a Service (RaaS) and cryptocurrency. These changes have unleashed an upward spike in ransomware attacks that are both sophisticated and disruptive, transforming it into a far broader national security, economy-wide, public health and safety threat.

Figure 1: High Impact Ransomware Attacks of 2021 and 2022

Date	Country	Organization	Impact
May 2021	USA	Colonial Pipeline	Temporary halting of all pipeline operations triggered panic buying of gas by consumers on the east cost of the U.S.
May 2021	Ireland	Health Service Executive (HSE)	Disruption lasting several days to hospital patient services that were already disrupted due to the Coronavirus pandemic.
June 2021	USA	JBS Foods	Disruption of the operations of the world's largest meat supplier (JBS paid an $$11 million ransom)
July 2021	W/Wide	Kaseya	Ransomware delivered into 800 – 1,500 customer environments via MSPs who use Kaseya's IT management software.
Feb 2022	Germany	Oiltanking	Disruption of inland oil and gas supply with terminals operating at limited capacity.

Source: HardenStance

The Latest Data Points to a Growing Threat

As shown in **Figure 1**, recent months have seen a marked increase in far-reaching societal risk arising from ransomware attacks on critical infrastructure like energy providers, food suppliers and healthcare providers. Some data points testifying to the growth of the problem and how seriously leading western governments are finally taking it, are also shown below:

Two of the most compelling data points arise from the recent February 9th, 2022, Joint Advisory by the U.S, UK and Australian governments. These are as follows:

- The UK government states in this Advisory that it "recognizes ransomware as the biggest cyber threat the country faces." Many national, regional and global industry surveys point to a lot of information security professionals taking the same view in relation to their own organizations.
- The U.S government states its cyber security agencies have seen ransomware incidents affect 14 out of the country's 16 critical infrastructure sectors. In a March 2022 'Flash' notice the FBI went further. It stated it has identified at least 52 entities across 10 critical infrastructure sectors affected by RagnarLocker ransomware. In addition the Cyber Peace Institute states at least 39 ransomware groups attacked the healthcare sector across 27 countries between July 2020 and December 2021.

In the February 2022 Joint Advisory, the UK government recognizes ransomware as the biggest cyber threat the country faces.

The FBI points to $6.9 billion losses in 2021

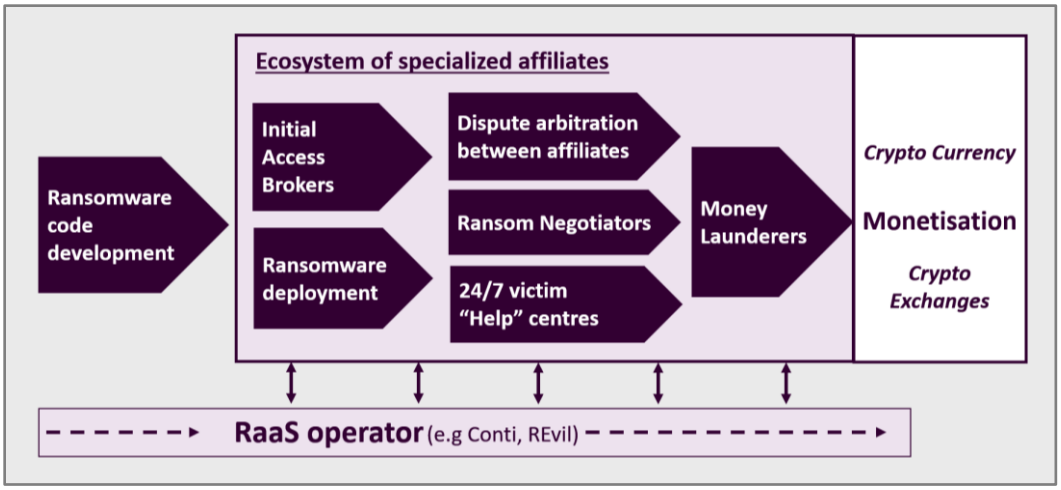
The next three data points arise from an October 2021 report by the U.S Treasury's Financial Crimes Enforcement Network (FinCEN) as well as from FBI and Security and Exchange Commission (SEC) filings in the U.S:

- The FinCEN report cited 635 Suspicious Activity Reports (SARs) just in the first half of 2021. This was up 30% on the 437 SARs for all of 2020.
- The FBI's latest Internet Crime Report estimates potential losses from cybercrime of $6.9 billion for 2021, up 64% on 2020.
- Having suffered a ransomware incident in October 2021, the Sinclair Broadcast Group said it paid no ransom and was able to restore its network from backups, but some disruption impacted revenues and expense, according to an analysis of its SEC filing undertaken and published by IDG's CSO Online on March 17th, 2022. According to CSO: "the incident resulted in a $63 million loss of advertising revenues for the broadcast segment in the fourth quarter and $11 million in remediation costs. After potential insurance reimbursements, the company estimates that the cyber incident will have resulted in approximately $24 million of unrecoverable net loss."

There follow four more data points for the money that ransomware gangs are making:

- In June 2021, when it arrested key members of the Clop gang in Kiev, Ukraine's national police estimated monetary damages the gang had inflicted at $500 million.
- In November 2021, the US Treasury Department stated that the REvil ransomware group had generated $200 million in ransoms.
- According to Coveware, the average ransom payment reached more than $300,000 in Q4 2021, up from just over $150,000 in Q4 2020, and around $90,000 in Q4 2019.
- JBS Foods is known to have paid a ransom of $11 million in June 2021.

Figure 2: The Rise of Ransomware as a Service (RaaS)



Source: HardenStance

The Efficacy of the Ransomware Ecosystem

Most ransomware attacks are not carried out by a single threat actor now but by collaboration between specialized affiliates working together across a highly developed ecosystem. Two of the most successful threat groups, REvil and Conti, now leverage these ecosystem partners according to the force multiplier that is now referred to as a Ransomware as a Service (RaaS) business model (see **Figure 2**).

Gaining access to victim networks is increasingly carried out by specialist Initial Access Brokers (IABs).

Gaining access to victim networks is increasingly carried out by specialist Initial Access Brokers (IABs). The Photon Research Team, Digital Shadows' external-facing security research team, observed a 57% growth in the number of IAB listings advertized in cybercriminal forums compared to 2020. The actual deployment of the ransomware into the specific customer environment is then done by different groups. Ransomware gangs have long operated "Help Desks", some of which do a good job of enabling victims to unlock and recover their data, although many do not. Over the last year or two, specialist service providers have sprung up to add value to this ecosystem. Some are carrying out ransom payment negotiations between victims and gangs; others are undertaking payment dispute arbitration between threat actor partners.

A second force multiplier driving this ecosystem is the growth in the crypto currency market. This enables ransomware gangs to draw down on their money off the books and in a way that is very difficult to trace. The price of a bitcoin was $10,700 in September 2020. It rose to $61,374 in October 2021 before falling back to $41,896 in March 2022. There were 13.3 million verified users of crypto currency exchange Coinbase in November 2017. That reached 89 million at the end of 2021. The development of the RaaS model – accelerated by the growth in the crypto currency market – introduces tremendous efficiencies, driving faster innovation by specialized providers. It provides phenomenally straightforward and rapid monetization for cyber criminals – there's no need for any secondary transaction on the sale of personal data or buyer of an infected host. The highly decentralized market structure also makes attribution of an attack to a specific gang very difficult.

TTPs Are Adapting and Evolving Accordingly

Organizations can expect the Tactics, Techniques and Procedures (TTPs) of ransomware gangs to continue evolving at pace, driven by the scale, efficiency and agility of the ecosystem. TTPs will also now be shaped by an additional factor - whatever form that ends up taking – in the form of the response of the Russian government and Russia's cyber threat actors to the country's deep isolation from the global economy.

This section looks first at what we might expect to see throughout the remainder of 2022 in terms of the modus operandi of Russia-based ransomware operators in particular. More broadly, it then looks at ransomware attack trends with respect to the balance between random and hands-on-keyboard attacks; the acceleration of 'double-dip' extortion; the targeting of Managed Service Providers (MSPs); and exploitation of new working patterns arising from the Coronavirus pandemic.

An uncertain outlook for the TTPs of Russia-based gangs

An uptick in cyber-attacks against western organizations to support Russia's objectives in Ukraine was widely anticipated. As of the time this White Paper was released, however, so far Russia has shown restraint in the cyber domain of the kind it has not shown on the ground in Ukraine.

Expectations of intensified cyber-attacks on western targets were heightened, among other things, by a message posted by the Conti ransomware group the day after the invasion began. Verified as genuine by researchers, Conti's post announced "full support of the Russian government", promising to "strike back" against the critical infrastructure of anyone who "organizes a cyber attack or any war activities against Russia."

Cut off from financial markets and starved of cash, the Kremlin could direct its intelligence agencies to copy North Korea's playbook and start large scale hacking for profit.

Days later, however, a Ukraine-sympathizer among Conti's anonymous associates retaliated by stealing and leaking the group's source code and internal chat logs. Hopes that this internal strife might be a substantial blow to the group were quickly dispelled by a March 7th report in CyberScoop. This pointed to two brand new Conti breaches of US companies, with several experts quoted confidently asserting that the spat was no more than a minor setback for Conti.

Just a couple of weeks into this war, with the full impact of sanctions still to be felt, the evolution in the TTPs of Russia based groups is highly uncertain. Consistent with the severity of the threat identified by the UK, US and Australian government advisory of February 9th, there are certainly no grounds to believe that the risk from Russia-based ransomware threats will diminish in the near to medium term.

Cut off from financial markets and starved of cash, the Kremlin could direct its intelligence agencies to copy North Korea's playbook and start large-scale hacking for profit. Equally, Russia could direct cyber operations to just lock up the critical data of western organizations without even offering to decrypt for a ransom. A hybrid approach is possible – permanently paralysing critical infrastructure without offering decryption keys while monetizing attacks on other organizations via a ransom demand. All these scenarios would substantially raise the risk from ransomware. Such opportunity as there may have been for constructive "ransomware diplomacy" as posited when Russian authorities' arrested REvil gang members in January 2022 is unlikely to materialize now.

Growth in far more impactful 'hands-on-keyboard' attacks

The first wave of ransomware attacks installed malware onto one single machine. Quite a lot of Antivirus solutions can still protect against this older ransomware. A key characteristic of changes in attack types in the last couple of years is the rise of so-called 'hands-on-keyboard' attacks whereby the first machine penetrated is just the first foothold in the attack campaign. With these newer generations of ransomware, attackers are then able to go on and move laterally within the organization and encrypt substantial parts of the organization's extensive infrastructure, wreaking a lot more havoc. Recorded Future reckons hands-on-keyboard attacks reached 65,000 in 2020.

From double to triple and quadruple extortion

In November 2019 the Maze ransomware group created a leak site. It threatened its ransomware victims who were hesitating or refusing to pay with leaking their data, not just locking it up. Many consider this the first 'double extortion' ransomware attack.

In the last two years this technique has evolved to triple and quadruple extortion whereby attackers are also layering in a threat of a DDoS attack and/or reaching out to a victim's customers to try and get them to apply pressure on the victim to pay up to avoid their data being leaked. In its 2022 Global Threat Report, CrowdStrike cites an 82% increase in ransomware-related data leaks during 2021 - 2,686 compared to 1,474 in 2020. Whereas in the past a world class back-up procedure might make it unnecessary to even consider paying a ransom as well as enable a comprehensive recovery, these additional extortions are layering new risks that great back-ups alone won't mitigate.

Penetrating an IT management software provider opens up access to dozens, hundreds or thousands of customers for ransomware gangs via the MSPs that use them.

A new focus on targeting MSPs to reach hundreds of victims

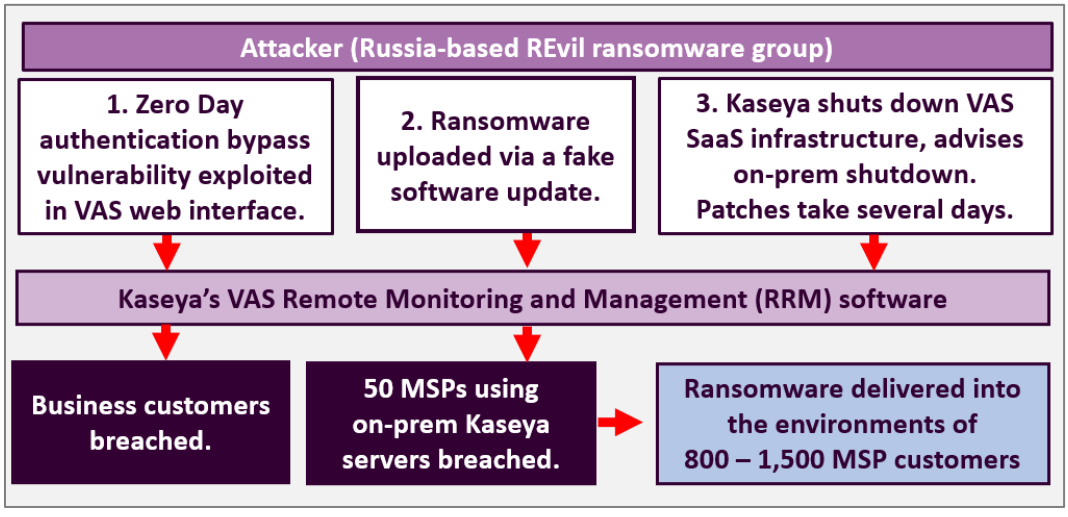
The Kaseya breach, first cited in **Figure 1**, is detailed in **Figure 3.** This was a hugely consequential attack. It exploited a zero-day authentication vulnerability in the software of this IT management software provider to deliver ransomware into the environments of between 800 – 1,500 unique customers via all the MSPs that use Kaseya. The SolarWinds breach didn't use ransomware but the reach into customers that it provided via SolarWinds own MSP arm, accounted for a sizable portion of the aggregate level of harm inflicted by that attack too.

Penetrating an IT management software provider opens up access to dozens, hundreds or thousands of potential victim organizations for ransomware gangs via the MSPs that use them. It's so much easier than having to gain access to each one individually. In their joint cybersecurity advisory of February 9th, 2022, cyber security authorities in the U.S, Australia, and the UK assess "there will be an increase in ransomware incidents where threat actors target MSPs to reach their clients."

Exploitation of the remote working legacy of the pandemic

Though not a force multiplier like the rise of RaaS and the cryptocurrency ecosystem, the coronavirus pandemic has been helpful to ransomware gangs in terms of heralding a seismic change in remote and hybrid work patterns. This has both disrupted and stretched the resources of IT and information security teams and greatly increased the threat surfaces of organizations. Hence why, along with software vulnerability exploits,

Figure 3: A Simplified Anatomy of the Kaseya Ransomware Attack



Source: HardenStance

phishing and stolen Remote Desktop Protocols (RDP) credentials are the three most common ways that ransomware attackers are gaining initial access to victim networks. This is according to several authoritative sources, including the February 2022 Joint Advisory released by the governments of the UK, U.S and Australia.

As well as expecting more from law enforcement, organizations should expect that governments and their regulators will do more to hold all enterprises accountable for aspects of their ransomware defence.

Law Enforcement Responses from Governments

As with other aspects of this new era of ransomware risk, an understanding of how government policy responses are affecting the landscape can be divided into the months leading up to the February 24th invasion of Ukraine and the weeks after.

The formation of the U.S. led Ransomware Taskforce at the end of 2020, and the subsequent inclusion of a first-ever explicit commitment to act on ransomware in the text of the G7 Communiqué in June 2021, marked the start of new era. Rather than leaving victim organizations to largely deal with the problem by themselves, western governments finally decided to direct law enforcement to give ransomware a higher priority, deepen international cooperation, and intervene to disrupt the ecosystem.

As shown in **Figure 3**, this commitment has yielded significant results. In the nine months since the G7 Communiqué there have been several arrests of ransomware gang members and sanctions have been imposed on some cryptocurrency exchanges. The FBI even managed to retrieve $2.3 million of the ransom paid by Colonial Pipeline. These disruptive actions by governments should certainly be welcomed – and more of them should be expected. However it's also important to recognize their limitations as well as anticipate the broader implications of greater government intervention in the market.

Criminal cyber gangs are agile, distributed and difficult to disrupt. Arresting and imprisoning leading members may only create a temporary disruption in activity. Moreover there are also a number of key safe haven countries that aren't likely to go obstructing ransomware gangs operating within their borders any time soon. These are countries like China, North Korea, Iran and Russia (for political reasons) as well as

Figure 4: Law Enforcement Actions to Disrupt Ransomware Gangs

Date	Country	Govt Agency	Action Taken
May 2021	U.S	FBI	Recovery of $2.3 million of the ransom paid by Colonial Pipeline to DarkSide cybercrime group.
June 2021	Ukraine	National police	Key members of Clop ransomware gang arrested.
Sept 2021	U.S	Treasury Department	Sanctions on Russia-based cryptocurrency exchange Suex for facilitating ransomware payments.
Nov 2021	Multiple	Europol	7 REvil & GrandCrab gang members arrested in South Korea, Romania, Ukraine as part of a 17-country operation.
Nov 2021	U.S	State Department	Sanctions imposed on Chatex cryptocurrency exchange for facilitating ransomware transactions.
Nov 2021	U.S	State Department	Offering up to $10 million for information leading to the identification or location of members of the REvil gang.
Jan 2022	Russia	FSB	14 members of the REvil gang arrested in Russia.
Jan 2022	Ukraine	National Police & Security Service	The fifth in a series of arrests of suspected ransomware gang members dating back to February 2021. Individuals suspected of affiliation to eGregor, Clop and REvil gangs.
Mar 2022	U.S	Justice Department	Maksim Berezan, a member of Russian crime gang, DirectConnection, sentenced to 66 months in prison and ordered to pay $36 million in restitution to his victims.

Source: HardenStance

countries like Kenya and Nigeria (more for reasons of insufficient prioritization and limited law enforcement resources). The same applies to crypto currency exchanges. Sanctioning them can create more - even a lot more - friction in the ransomware business model. But again it only takes a few actors to be able to access a few exchanges for cyber criminals to navigate their way around law enforcement barriers.

Given the above, it shouldn't need saying that organizations can't in any way view the stepping up in government engagement as a reason to offload responsibility for ransomware protection onto government. Actually, the reverse is the case. As well as expecting more from law enforcement, organizations should expect that governments and their regulators will do more to hold all enterprises accountable for aspects of their ransomware defence in the interests of helping defend all organizations.

The marked rise in ransom payments over the last couple of years has made a big contribution to the hardening of the cyber insurance market, whereby margins are tightening even as premiums rise steeply.

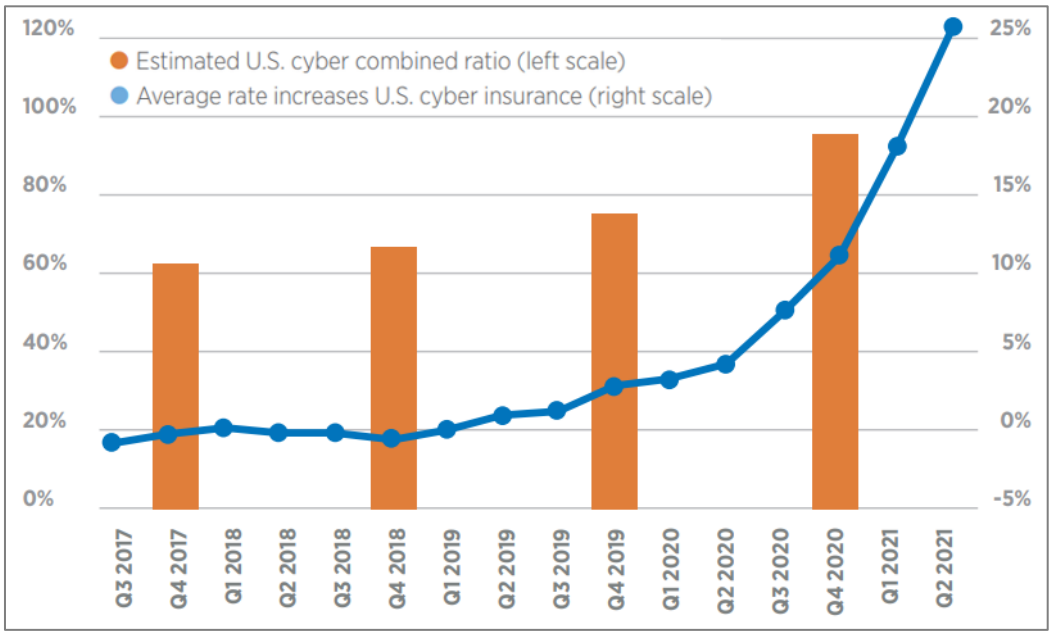
Actions may include more stringent requirements with respect to reporting on ransomware incidents and the sharing of threat intelligence as well as potential restrictions on the payment of ransoms. This would affect the cyber security posture of organizations with a presence in countries impacted by these regulations.

Russia's invasion of Ukraine is more likely to accelerate rather than slow the momentum of those governments that have started down this more interventionist path. For example, more sanctions on crypto currency exchanges are surely more likely now. The same is likely true of controversial policy prescriptions for curtailing or even banning the payment of ransoms. These were in the very early stages of gaining some traction with policy makers in one or two countries during 2021, albeit still nowhere close to making it into legislation. Russia's invasion has potential to alter this, though. It was one thing for the private sector to make the case for its right to appease Russian cyber gangs by paying their ransom demands before February 24th. That case may get a less favourable hearing from now on.

The Cyber Insurance Market's Verdict Is In

The marked rise in ransom payments over the last couple of years has made a major contribution to the hardening of the cyber insurance market, whereby margins are tightening even as premiums rise steeply. This is depicted in **Figure 5**. The blue line can be understood intuitively. It depicts the steep percentage increase in U.S cyber insurance premiums. The orange bars require explanation. They represent an estimate

Figure 5: Despite Rising Premiums, Cyber Insurance Profitably is Tightening



Source: Arthur J. Gallagher and Co/Standard & Poor's Financial Services LLC

of the 'combined ratio' for cyber insurance in the U.S. This is the ratio of insurance company losses and expenses to revenue. **Figure 5** shows this ratio growing over the last three years, meaning that the margins in cyber insurance are narrowing. The implications are clear. There's more demand chasing less money, which is driving an overall tendency to substantially increase premiums and better scrutinize policy terms. In France, for example, AXA's new policies no longer pay a ransom. Providers are setting more stringent qualifying conditions, requiring that organizations meet higher standards of baseline cyber security as a condition of being sold a policy.

Key Priorities for Updating Cyber Security Posture

Taking account of both the upside of government interventions to disrupt ransomware gangs and new risk arising from the war in Ukraine, ransomware poses a bigger threat to most businesses now than it did a year ago. It's not clear whether current government actions will materially bend the rising curve in terms of the volume or efficacy of ransomware attacks. Given what could happen, triggered by Russia's new pariah status, current actions may not even bend the curve at all.

Protecting against ransomware is an integral part of an organization's broader cyber security posture. Comprehensive patching, blocking phishing emails and reducing the scope for credential stuffing is pivotal to defending organizations but it's equally critical to defending against most other high impact cyber attacks too. It's beyond the scope of this White Paper to recommend a comprehensive approach to defending against ransomware or cyber security risk more broadly. Instead, this section draws on the insights shared on recent changes in the market landscape to highlight five key measures which are critical to mitigating these new or heightened risks.

There is just too much embedded trust in the relationships between IT organizations, their MSP partners and the critical management software platforms they use.

1. Review cyber insurance needs (and how policies are chosen)

The hardening of the insurance market renders reliance on insurance compensating for an attack, while investing a bare minimum in prevention, even less viable than ever. Ironically, organizations should arguably welcome this development as an additional incentive to harden their overall security posture.

Organizations that can demonstrate a strong commitment to their cyber security posture – who can prove themselves to be a good risk – will continue to have no problem finding high quality insurance providers that are committed to partnering and providing excellent coverage, albeit they may still see premiums increase somewhat.

Given the tightening in policy conditions – especially the mapping of policy terms to a provider's expectations of an organization's baseline cyber security – CISO teams should be involved in procuring insurance now. CFOs, Chief Counsels and risk managers should no longer be making these decisions independently. Organizations that can't meet baseline provider requirements will find it a harder to get good quality insurance and will see their premiums increase significantly. Organizations that can't meet even minimum standards are starting to become uninsurable – no provider will insure them. And if you can't get insurance, that just transfers cyber risk onto the organization's own books. In line with sanctions on Russia, organizations should also consider the possibility that insurance companies may be prohibited from paying ransoms by the time they are taken down by a ransomware gang.

2. Mitigate risk from third party MSP partners

Organizations need to do more to defend against third party supply chain risk in general but as the Kaseya attack showed, and as leading national cyber security agencies have very recently warned in February (see page 6), greater scrutiny of operational interactions with MSP partners should be prioritized. There is just too much embedded trust in the relationships between IT organizations, their MSP partners and the critical management software platforms they use.

Clients that are attached to these software vendors' servers tend to perform whatever task is asked of them. Typically, hardly any verification is carried out on those instructions. Introduction of greater – ultimately continuous - contextual verification of commands according to Zero Trust principles will reduce exposure to ransomware and other attacks.

3. Harden operational processes around RDP

To mitigate the risk of RDP being exploited in today's more dynamic, hybrid working environment, it has to be properly secured and monitored. The first part of a section on this in the UK, US and Australia government's joint cyber security Advisory of February 2022 recommends the following:

- Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure.
- After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources and require MFA to mitigate credential theft and reuse.
- If RDP must be available externally, use a virtual private network (VPN), virtual desktop infrastructure, or other means to authenticate and secure the connection before allowing RDP to connect to internal devices.
- Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts to block brute force campaigns, log RDP login attempts, and disable unused remote access/RDP ports.
- Ensure devices are properly configured and that security features are enabled.
- Disable ports and protocols that are not being used for a business purpose

Organizations that are not yet making explicit provision for securing and backing up both their cyber insurance and incident response documents offline as well as online should do so.

4. Review Incident Response plans

A heightened readiness by governments to intervene and regulate the market has potential to change the mix of legal requirements and options a management team has at its disposal when responding to a real-life ransomware attack under intense pressure. Examples include new requirements or restrictions relating to incident reporting and paying ransoms. This must start to be factored into incident response plans.

Organizations may be hesitant to report an incident and engage with law enforcement unless they're bound to by law. But even voluntary cooperation can bring its own rewards. One example is in terms of securing approval to pay a ransom or, as with the case of Colonial Pipeline, securing law enforcement's help in clawing back some or all of a ransom payment after the transaction has been made.

Organizations that are not yet making explicit provision for securing and backing up both their cyber insurance and incident response documents offline as well as online should do so. By viewing insurance documents, attackers can learn the exact amount of ransom they should demand. Immediately following a ransomware attack, defenders may try accessing their attack response documents only to find that they too have been encrypted by the attack. The reach that attackers can gain into an organization now also means that they are increasingly encrypting or destroying on-line backups to drive victims to pay the ransom. Hence offline back up is required, whether via a disaster recovery network, a cloud provider, tape or another solution. Gold images of critical servers should also be backed up so systems can be quickly rebuilt following an attack.

5. Consider total costs before deciding whether to pay a ransom

As shown, the volume of ransomware attacks is growing as is the severity of their impact. As part of their incident response planning, organizations must determine their position as regards whether or not to pay a ransom. No-one wants to give criminals their money for threatening them but, depending on the circumstances, many of us may be able to justify it as the lesser of two evils.

There are three important things to consider. The first is to take a holistic view of total ransomware recovery costs and where a ransom payment fits into that. Paying a ransom may get some of your data back. In some cases it might even get all of it back. But paying may make you more vulnerable to a second attack. It also won't protect you against incurring other costs. Ransomware often leaves data and infrastructure permanently depleted or destroyed or temporarily inoperable which can take months to remediate. Data also has to be verified to ensure its integrity hasn't been compromised.

The reality of what the total costs really are is often a lot more complex and nuanced than it first appears.

Remediation, lost revenue, legal and other costs can easily make up 80% of the costs of recovering from a ransomware attack. The ransom itself may be no more than 20% of the total. These costs must be met irrespective of whether the ransom is or is not paid. The reality of what the total costs really are is often a lot more complex and nuanced than it first appears – and it's the reality that must be considered in a decision on whether or not to pay.

The second is to analyse the available alternatives to paying the ransom. Organizations like No More Ransom make decryption keys to certain malware groups freely available; in other cases, law enforcement, network defence, or incident responders might have a key. In those cases, you do not need to pay the ransom. While acknowledging the time pressures to restore business operations, undertaking some level of due diligence will help ensure that you are making the best decision under the circumstances – and that you can support that decision later.

The third issue to consider is the potential impact of any new regulations that might limit or even ban the payment of ransoms by organizations or their insurers. This is even more relevant now in light of sanctions on Russia. ■

About the Sponsors

The sponsors of this White Paper are the Cyber Threat Alliance, Juniper Networks, Resilience Insurance and Security Scorecard.

About Cyber Threat Alliance

The Cyber Threat Alliance (CTA) is a 501(c)(6) non-profit organization that is working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field. We take a three-pronged approach to this mission:

1. Protect End-Users: Our automated platform empowers members to share, validate, and deploy actionable threat intelligence to their customers in near-real time.

2. Disrupt Malicious Actors: We share threat intelligence to reduce the effectiveness of malicious actors' tools and infrastructure.

3. Elevate Overall Security: We share intelligence to improve our members' abilities to respond to cyber incidents and increase end-user's resilience.

CTA is continuing to grow on a global basis, enriching both the quantity and quality of the information that is being shared amongst its membership. CTA is actively recruiting additional cybersecurity providers to enhance our information sharing and operational collaboration to enable a more secure future for all. For more information about the Cyber Threat Alliance, please visit www.cyberthreatalliance.org

About Juniper Networks

Juniper Networks is dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality. Additional information can

be found at Juniper Networks www.juniper.net or connect with Juniper on Twitter, Linked In and Facebook

Resilience Insurance

Resilience provides comprehensive insurance coverage and patented cybersecurity products to protect mid-market companies. By bringing together security, insurance, and recovery, Resilience goes beyond risk transfer to help clients become cyber resilient.

Resilience Cyber Insurance Solutions, the cyber program manager of Intact Insurance Specialty Solutions—which is backed by the financial strength of Intact Financial Corporation—leverages Cyber Meteorology, a proprietary data-driven risk analytics platform, to provide highly targeted coverage, allowing for a superior claims experience. Resilience is backed by General Catalyst, Lightspeed Venture Partners, Founders Fund, CRV, Intact Ventures, Shield Capital, and Corey Thomas. Coverage offered through Lloyd's will be available through an approved cover holder. For more information: www.resilienceinsurance.com

Security Scorecard

Funded by world-class investors including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings with more than 12 million companies continuously rated. Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every organization has the universal right to their trusted and transparent Instant SecurityScorecard rating. For more information, visit www.securityscorecard.com or connect with us on LinkedIn.

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, OASIS, The GSMA and ETSI. HardenStance is also a recognized Cyber Threat Alliance 'Champion'. To learn more visit www.hardenstance.com