HOW TO RECOVER YOUR BUSINESS FROM A CYBER INCIDENT

It will come as little surprise that cyber incidents are on the increase with many big names being the victim of attacks including Colonial Pipeline [1] which, in June 2021, resulted in the company paying a 'ransomware' of $4.4 million (a portion of which, $2.3M, was subsequently recovered by the FBI) [2] and, in August 2021, the announcement of a data breach against T-Mobile USA which compromised the data of nearly 100M 'current, former and prospective' customers.[3]

In fact, cyber-crime is such big money now that the income from it would make it the 3rd largest country by GDP in 2021, worth over $6tn.[4] Concurrently, in 2020 there was a 238% increase on cyberattacks on banks as a consequence of COVID.[5]

And the stakes are getting higher all the time: a cyberattack in Germany on a hospital has been linked to the death of a patient.[6]

With such lucrative rewards possible, there is no shortage of motivation for cyber criminals to launch attacks on businesses they see as viable targets.

SUNGARD AVAILABILITY SERVICES®

Recently, Sungard AS hosted an industry roundtable to which we invited customers to ask them on how they are coping with the ongoing challenge of surviving complex cyber incidents.

In turn, we developed this whitepaper to demonstrate that it's not always how a company responds to an attack, but rather how being prepared ahead of one that can, ultimately, make a significant difference to successful outcomes should it ever suffer the misfortune of being hacked.

In this whitepaper we will discuss:

> The major threats and risks facing businesses today

> The rise of ransomware

> Adopting a three-layered approach to cyber resilience

> What vital data Is and what it isn't

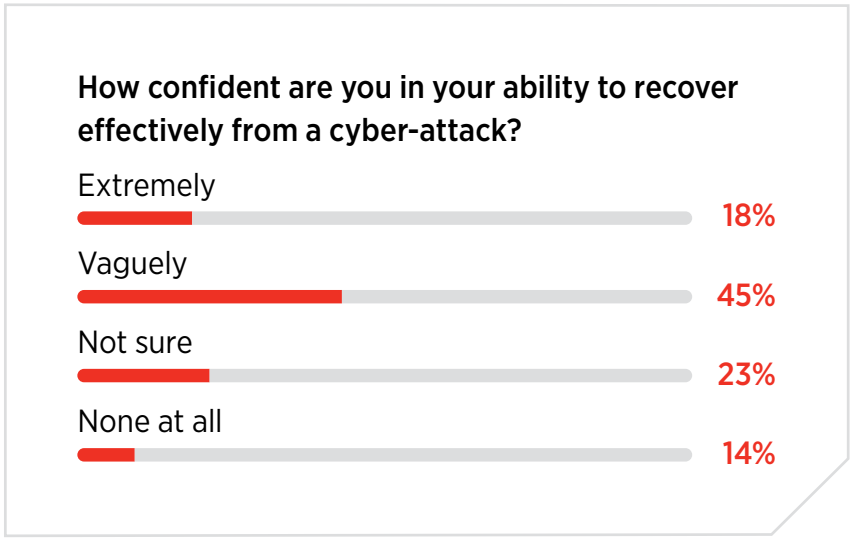
> Developing a program approach to cyber compromised data recovery

> Formalizing an approach to complex data recovery following a cyber incident

We will also be including the questions and results of these customer polls to provide readers with a real-life basis for how their peers are managing the threat of cyber-attacks today — and how to stop them tomorrow. //

The major threats and risks facing businesses today

To establish a baseline of how our customers perceive the threat of cyber-attacks today we first posed a very fundamental question:



The past 12 months has seen a pretty varied set of threats emerge; some with significant impact for their victims. For anyone who suffers a ransomware attack, let's not forget you are the victim of a crime.

A number of US Police Forces have been attacked, with the Washington DC Metropolitan Police and the NYPD both among the victims. The NYPD malware was introduced by a contractor whose PC had already been infected by malware – the contractor appears to have been completely innocent.[7] More chillingly, the Metropolitan Police Department suffered a network breach and the hackers first threatened then released sensitive data on police informants. The information gathered on criminal gang activity and police intelligence would be particularly damaging operationally speaking for any police force, let alone the one that covers the Washington DC area.[8]

In March 2021, a Russian in the USA working on behalf of criminals abroad pleaded guilty to attempting to bribe a Tesla employee to install malware on the network of the Tesla battery plant in Nevada. They offered the Tesla employee $1 million to play their part in this attack, but to his credit, the employee instead alerted Tesla management and the FBI who foiled the plot which unfolded as early as last August/September. The conspirator has since been charged and sentenced to incarceration in the US.[9]

These US examples show that threats can include staff and contractors, clearly in this case they were the 'good guys', but there are a number of ways into a network. This includes acknowledging that a technical brute force attack against increasingly good cyber defenses has a low probability of success. It's usually when specific vulnerabilities can be exploited—for example the VPN Server patching vulnerability that allowed hackers into Travelex,[10] amongst others—prove that technical attacks succeed.

The easiest way into a network is by exploiting employees and their emotions, routines, behaviours and, of course, their lack of general awareness of cyber security. Not many workers can recognize every sophisticated cyberattack. In the UK, there has been a huge proliferation of 'smishing." For example, fake SMS messages from Hermes, Royal Mail or DPD requiring the payment of a £2.99 delivery fee, which then leads to a call from the equally fake fraud department of your bank, encouraging you to move money immediately to a new account the fraudsters have set up. Or notifications from Deliveroo, Uber, any of the mobile phone providers, or even PayPal saying your account has been temporarily restricted due to suspicious behaviour. Similar scams involving COVID tests, checks, vaccinations, masks and so on are also very widespread.

The targets can be many and varied. Recently Northern Rail's ticket machines in the UK were victims of a ransomware attack.[11] In the recent Microsoft Exchange hack,[12] the NCSC estimated 7,000 email servers were discovered to be unsecured and only half of this number had been secured subsequently. Small and medium sized businesses are most affected, as these firms do not usually have significant IT security budgets.

The rise in ransomware attacks seems inexorable, and according to data from SonicWall,[13] the number of ransom attacks rose 60% in 2020 to $305 million, as hackers took advantage of the mass working from home movement and the vulnerabilities that opened up as a result.

The rise of ransomware

The latest trend (and growing rapidly) is Ransomware as a Service, which is basically pay-per-use malware created for extortion and compromise of data. This is nothing more than SaaS for the bad guys. Indications are that the Colonial Pipeline attack in the USA was executed using R-aa-S.

As Ransomware demands go up, so too does the cost of clean-up, doubling over the past year. According to Sophos, the average cost of a ransom situation is 10 times the ransom paid, and only one in 10 companies that pay a ransom get all their data back. [14]

In the UK, a recent survey by Cybereason has found that:

84%

of organisations that paid a ransom demand were hit again

61%

reporting significant loss of revenue. [15]

Why is Ransomware growing so fast? There are a number of factors.

1. Internationally available cloud infrastructure has grown exponentially, and this benefits businesses. Unfortunately, it also enables cybercriminal gangs to launch attacks from anywhere. The use of RaaS has exploited this fact, with the attackers looking to penetrate an organisation but using the franchisers' encryption tools, communications, ransom collection etc. for the payment of a percentage of the ransom. As a result, the attackers are not having to create bespoke tools each time they launch an attack and can benefit from the DEVOPS approach and expertise of the RaaS provider.

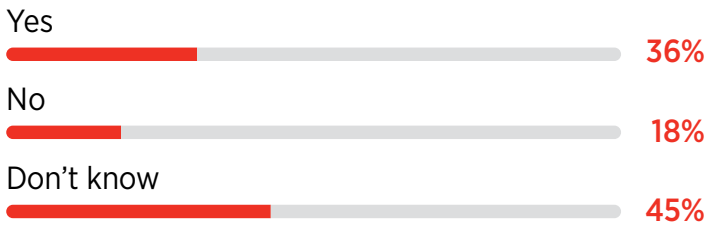
2. Hackers are also increasingly targeting critical infrastructure and supply chains. A hacker almost managed to poison a Florida town when he hacked into their SCADA that controlled the various chemicals in the water treatment facility. [16] Upon further investigation it was determined the plant had old software and poor security. The biggest attack recently on critical national infrastructure was, of course, the aforementioned Colonial Pipeline attack. Why are these sectors targeted? Largely because they have a very short window of acceptable downtime, they are providing very public services, and the media and politicians will be all over them in the event of an attack. This makes them more likely to pay up.

But there are some trends moving in the other direction, including some insurance limitations. Take cyber insurance premiums which increased by 27% over the last 12 months.[17] Insurers are demanding a much more robust approach to cyber security and if your company does not have sound foundations, it is unlikely to get affordable coverage. Even if you do have coverage, there are increasingly signs that you won't be able to use the insurance for the cost of the ransom payment itself. The French insurance company AXA recently announced in France that it would no longer pay out on ransom demands. [18] Payment of ransom demands is undoubtedly fuelling the industry, and we have also seen the first indications of a similar policy direction emerging in the US following the Colonial Pipeline attack.

Preventative measures are always a good starting point, and with increasingly more sophisticated cyber incidents. becoming the norm, it is now more important than ever to think about how your business could recover any cyber compromised data.

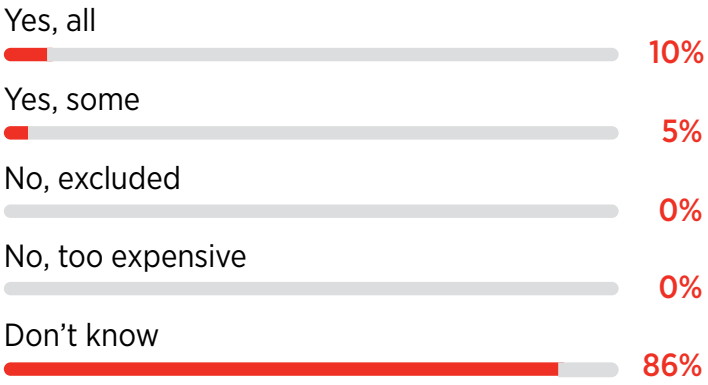
Our next poll asked if discussions around paying ransomware have ever been discussed in the workplace:

Have you, or your executive team, ever discussed whether you would pay a ransom demand?



A follow-on poll asked:

Would your insurance policy cover a ransom payment?



Adopting a three-layered approach to cyber resilience

Even when it comes to ransomware, there are, without question, ways in which these risks can be mitigated.

Preparation is key. This includes developing a three-layered approach to cyber resilience that include working with:

Additionally, having conversations with the leadership team over your insurance coverage and whether, in principle, they are opening to paying the ransom demand.

Working with the business teams allows companies to understand their priorities and this information will often be found in the Business Impact Analysis. Critically, however, the BIA does not often address the issue of Vital Data. For complex recovery, you do need to know what your Vital Data Assets are. Vital data is linked to the critical applications, which are in turn supporting the business-critical identified in the BIA.

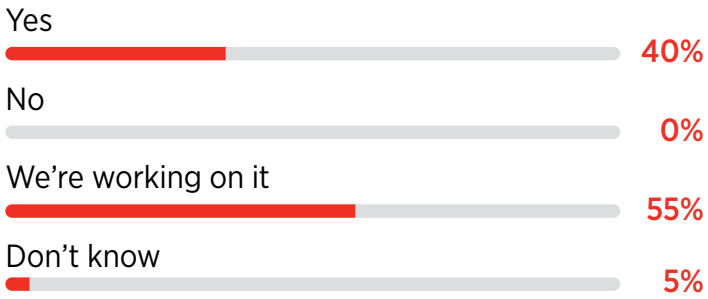
Finally, work with the IT and information security teams, including third party technology partners. Here you can ensure that plans are prepared that are tested, are coherent, are aligned with business needs and are well practiced by recovery teams.

Again, and because it can't be overstated, business preparation is key.

What vital data is and what it isn't

We next polled about vital data and customers' perceptions about what vital data is and what it isn't.

Do you understand what information is vital to the effective operation of your business?



IT Disaster Recovery (DR) is not the same thing as recovery of compromised data. Disaster recovery does not, in fact, equal data recovery. There are different use cases in play. Traditional DR, normally covered in DR runbooks, will focus on recovery of infrastructure, applications and network services when the Data Center has been compromised. Typically, RTO (Recovery Time Objective) will be achievable and hopefully no RPO (Recovery Point Objective) issues will be experienced as the data is all still present and accounted for.

However, Data Recovery following a cyber compromised event is a different matter. You will not know what your achievable RTO is and indeed whether the RPO can also be met. What is your last clean data point? How old? Is that data even relevant to the business anymore? Given the triage and investigation needed post cyber incident, it's practically guaranteed that you can't meet the RTO. Interestingly, this is one reason why some ransom demands are paid, because the company has no idea how long it will take them to clean up and restore their systems. It's not that they can't, it's that they just don't know how long it would take and what the business impact would be. In fact, the firm might have already gone under by the time they finish recovery.

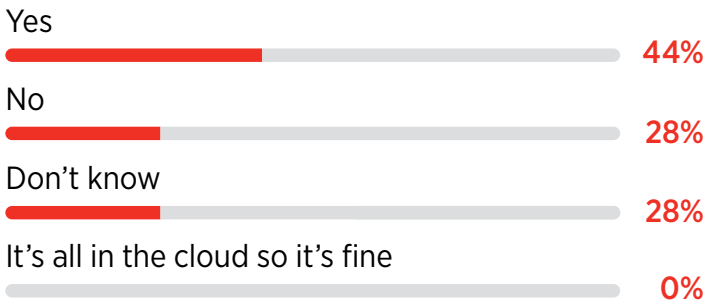
Some vital data might not even be in scope of the DR program. Think of an oil and gas company such as BP (British Petroleum). A vital part of its development work is identifying new fields for exploration and exploitation. This requires long term knowledge of geology and such analysis builds up vital data accumulated over many years. This will have a very long RTO because it's not needed within a month, or even six months, but it is critical to the company's ability to research, innovate and invest in new operations. So no RTO, not in scope of the DR program, but still vital data nonetheless.

An alternative use case is Amazon. What's on its shelves in a fulfilment centre 72 hours ago is probably irrelevant. So that data is vital and will have a very short RTO, but it really won't be that interested in old stock information for current operations. Its tactic in the event of loss of that data would be to re-inventory the shelves. If that data can't be recovered quickly they are not interested.

IT Disaster Recovery (DR) is not the same thing as recovery of compromised data. Disaster recovery does not, in fact, equal data recovery.

Our next poll question concerned how the loss of vital data affect the business:

Are you worried you would permanently lose some vital data in the event of a complex cyberattack, to the severe detriment of the business?



Developing a program approach to cyber compromised data recovery

What we are suggesting is a different approach to IT DR, that focuses on data protection — a program approach to cyber compromised data recovery.

First, you need to know what your vital data is. What's in scope and what are your requirements?

Chances are you will focus most of your resources on the Tier One data — that intersection where Confidentiality, Availability or Integrity scores highest in relation to your business critical activities. Your so-to-speak Crown Jewels will be stored in the inner vaults of the Bank of England, to co-mingle the analogy.

By tiering your data you will then be able to work out what technical solutions might be most appropriate for your firm. In any case, your goal is to protect your vital data.

There are a range of solutions available for safeguarding your Tier One data, but it will require a bespoke recovery case. This will involve the ability to isolate that data, store it in immutable format, off-network, use AI tools to scan for threats or compromise, and the ability to check it for cleanliness before restoring it to operational environments. Each firm will have different requirements and therefore there is no one size fits all approach.

Taking a program approach to this reduces risk and prepares the organisation to recover much more quickly from an incident. It provides firms with priorities for recovery activities and applies a known, tested plan that has been practiced frequently. For this to succeed, you will need to have suitable procedures in place that allow you to respond to the event — such as crisis and incident management, crisis communications, cyber run books, technical detection and forensic services, and so on. You will also need to be able to recover your vital data back into an operational environment, to minimise the business impacts, and reduce the overall risk to the business of being fatally holed beneath the waterline by the attack.

Because this is complex, you need to be able to prioritise and practice. Developing knowledge and familiarity with procedures through exercising and testing is essential, just as it is for any major disruption. You are likely to already practice your crisis and incident management procedures, probably as part of your overall BC program. In fact, you should look to incorporate cyber data recovery as one of your scenarios in exercising and testing. In other words, don't leave it to the day of the battle!!

Formalizing your approach to complex recovery

If you don't formalize your approach to complex recovery, it will always be down to best effort on the day of the event and that simply is no longer good enough.

REASONS TO FORMALIZE

- Cyber recovery is complex and requires a different use case to traditional IT DR approaches
- It's a combined effort, from top to bottom in the organisation. This is definitely not an infosec team problem
- Regulators and insurance might well be driving changes in behaviours
- You can't secure everything and you should expect to be attacked. Therefore this drives the need to take a balanced program approach to managing cyber risk and ensuring cyber resilience
- Exercising and testing builds confidence and experience

It may be an over-simplification of the facts but when it comes to ransomware, there are no guaranteed defenses available today to universally prevent its insurgency.

Fortunately, by taking a holistic approach to the ransomware threats and applying some of the best practices we've outlined here, you can "buy down" the risk of a failed data recovery effort. So, identify your Vital Data Assets, Protect them with proven backup technologies, monitor them to detect anomalies (since their integrity is essential), develop threat focused plans to guide your Response to an actual ransomware situation, and ensure it will all work at time of Recovery by conducting exercises and tests that validate you plans, capabilities, and teams.

While there is no silver bullet when it comes to recovering data compromised by cyberattacks/ransomware, by being prepared you can successfully manage the changing face of DR and, hopefully, before a data-compromising cyberattacker sets your organization in its sights.

www.sungardas.com

If you are calling from
North America contact us at:

+1 (866) 714-7209

If you are calling from
EMEA contact us at:

+44 (0) 808 238 8080

Citations:
(1) bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password (2) apnews.com/article/technology-business-government-and-politics-8e7f5b297012333480d5e9153f40bd52
(3) theregister.com/2021/08/16/in_brief_security/ (4) cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (5) zdnet.com/article/covid-19-blamed-for-238-surge-in-cyberattacks-against-banks/
(6) wired.co.uk/article/ransomware-hospital-death-germany (7) cisomag.eccouncil.org/nypd-infected-by-a-ransomware-accidentally/ (8) apnews.com/article/police-technology-government-and-politics-1aedfcf42a8dc2b004ef610d0b57edb9
(9) bbc.com/news/world-us-canada-56469475 (10) echcrunch.com/2020/01/02/travelex-malware/ (11) reuters.com/world/uk/uks-northern-rails-self-service-ticket-machines-hit-by-ransomware-cyber-attack-2021-07-19/
(12) zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/ (13) blog.sonicwall.com/en-us/2021/06/cybersecurity-news-trends/ (14) forbes.com/sites/daveywinder/2021/05/02/ransomware-reality-shock-92-who-pay-dont-get-their-data-back/?sh=7c23ac90e0c7 (15) retailtechnologyreview.com/articles/2021/06/29/new-cybereason-ransomware-study-reveals-true-cost-to-business/ (16) bbc.com/news/world-us-canada-55989843
(17) itpro.com/security/cyber-security/360131/cyber-insurance-premiums-increased-by-a-third-in-the-last-12-months (18) insurancejournal.com/news/international/2021/05/09/613255.htm

About Sungard Availability Services
Sungard Availability Services provides managed IT services, information availability consulting services, business continuity management software, and disaster recovery services.

Trademark information
Sungard Availability Services is a trademark or registered trademark of SunGard Data Systems or its affiliate, used under license. The Sungard Availability Services logo by itself is a trademark or registered trademark of Sungard Availability Services Capital, Inc. or its affiliate. All other trademarks used herein are the property of their respective owners.

SUNGARD
AVAILABILITY
SERVICES®