

► Cyber and Malware:  
Protection and Recovery for  
Pharmaceutical Companies



## MANAGING RANSOMWARE RISKS IN THE PHARMACEUTICAL SECTOR

Cyber-attacks have made the headlines far too often in recent years, with malware having a significant impact. Media reports regularly put the cost to businesses, including pharmaceutical companies, into the hundreds of millions.<sup>1</sup>

Malware is on the rise, and it's no surprise, with the prevalence and ease of access to criminal toolkits, often referred to as Ransomware as a Service, or RaaS. This makes targeting a single organisation on multiple fronts much easier, and attacks can be made even more effective when combined with social engineering tactics.<sup>2</sup>

Attacks are not limited to crypto-lockers, with malware such as Not-Petya measuring its success by completely taking systems down and making them un-bootable. Statistics indicate<sup>3</sup> that WannaCry has remained active for an extended period, and while it is easy to dismiss if you escaped it due to timely patching, many new government and state actor exploits are leaked on a regular basis. Sites like WikiLeaks and Shadow Brokers are two well-known sources, but there are many more on the dark web.

Commvault has helped many customers recover from this situation, but a self-perpetuating malware attack vector is unlike a traditional disaster. This white paper looks at what we learned about recovery after a cyber/malware/ransomware attack.

When a 'normal disaster' hits systems, sites or networks, it has a big impact, but it is generally localised. Once successfully deployed inside your environment, malware spreads in a subversive way, often corrupting whole swathes of critical systems and services before alerting its presence.

## THE RANSOMWARE CHALLENGES FOR PHARMACEUTICALS

Every business has 'red line' data that it can't risk losing, and the Pharma sector is no different. Drug trial data is highly regulated and can spike in value as new uses are discovered for existing drugs; losing this data can put drug development back years, costing many millions of dollars. ERP systems are critical for production, and downtime can have a huge impact on the bottom line, not to mention leaving patients without access to life saving drugs, increasing the potential for expensive law-suits to follow.

### "DEFENCE IN DEPTH" AND PATCHING

"Defence in depth" – employing many layers of defensive tactics – is still the best approach, but is only effective when used in conjunction with robust processes for patching operating systems, applications and hardware.

To date, many of the attacks that have made the headlines have used relatively well-known vulnerabilities, and organisations that have strong patching regimes have avoided infection. The challenge is that the 'Ransomware as a Service' business model employed by cybercriminals seeks to weaponise these security holes at a faster rate, which increases their potential for success, and thereby their profits. A report by Cisco<sup>4</sup> highlights that the median time available for security staff to react to an attack in 2018 is down to just 4.6 hrs, a drop from nearly 40hrs in 2015.


Many organisations affected by WannaCry and Not Petya lost critical services such as Active Directory, hindering authentication and slowing down system recovery processes.

1 Security Week, August 2017

2 The Social Engineer Organisation

3 Sophos 2018 Malware Forecast, November 2017

4 The Cisco 2018 Annual Cybersecurity Report, The Cisco Newsroom, February 2018



While no 'zero days' exploits have yet made it into a viable ransomware attack, many experts believe it's only a matter of time before it does. Patching can be hindered by change controls, which can affect users as well as production systems. For this reason, a pragmatic approach and balance is required between fast-patching and reliability. This is another reason why rapid recovery systems should be necessary, and why patch compatibility with backup systems should be the first thing on patch check-lists.

## YOU CAN'T PATCH HUMANS

One area that can't be patched are humans, who are the number one target for attackers. Unfortunately, attackers' approach in this area is becoming ever more sophisticated, with multiple marks identified and prayed upon within a single company. This kind of targeted attack will use intelligence gained from many sources, and is even capable of throwing up very specific, personal data that can entice the installation of malicious code by even the most vigilant and well-trained people.

The other human factor comes into play with regard to practical design. Commvault support have encountered questionable short-term decisions that have had significant, undesirable impacts. For example, some systems have the ability to create their own backups of critical files outside of company-standard backup system. Putting these files on the server's own C drive renders them useless in the case of ransomware, and potentially delays the recovery of other services.

## LOST DR PLANS AND PRIORITY SWITCHING

One serious issue seen at a pharmaceutical company was the complete loss of their system blueprints and disaster recovery plans, which were only kept digitally. This is a serious problem, however, even where the DR plans remained accessible, the scale of the outage was such that those plans offered only limited practical assistance.

As events unfold, the broad scope of a serious attack means priorities constantly shift, and this is not helped by staff and management who are put under significant pressure, and are often hindered further by the loss of communications systems. Management shift changes can also lead to priority changes, as do uncontrolled demands from the business. Long hours and fatigue also cause basic errors that have a direct and significant impact along the way.

The net of all of these challenges is that outages continue for much longer than necessary, which can be measured in days, not just hours.

## LEVERAGING AI FOR EARLY DETECTION

Due to its nature, stopping Ransomware is nearly impossible to do, so spotting it early is the next best alternative. Desktop computers are the usual entry point, and anti-virus software can help identify data being encrypted or the injection of suspicious code into the OS boot data. Unfortunately, this is getting increasingly harder to spot, so having multiple ways to detect an attack early has become increasingly important.

Many organisations affected by WannaCry and Not Petya lost critical services such as Active Directory, hindering authentication and slowing down system recovery processes.

Commvault employs a 'honey pot' approach to attract encryption style malware, which will alert administrators to an attack as soon as this is detected. AI is also used by Commvault to track suspicious activity, but rather than send false positives, it is balanced against normal user activity before a warning is flagged. In addition to this anomaly alert, Commvault also automatically extends the retention of any backup data about to be expired, just in case the malware has an extended operation period before the payload runs.

## BECOMING RECOVERY READY

No-one wants to resort to backups in the event of a Ransomware attack, but this is a reality that happens all too often. In the very worst cases, the backup systems themselves can be compromised, meaning little short of cracking the encryption keys or paying the ransom to regain access to the data again. Clearly, the latter is not recommended and provides little guarantee where criminals are concerned.

This means that to become 'recovery ready', you must ensure your backup system itself is as secure as possible from being affected. Commvault provides many built-in ways to ensure this is the case, which is switched-on by default. Additional protection can be afforded by these considerations:

- Retaining tape. While many organisations want to remove tape due to high associated costs, it does provide true, offline copies that cannot be affected by any current malware
- Using multiple operating systems as media servers. Malware that can jump OS is very rare, so mixing Windows and LINUX/UNIX backup servers affords extra protection for your data
- Create offline copies in the cloud. Any data that is online is at risk, so creating data copies that are offline when complete provides added defence

Of course, recovery readiness is not just about creating a secure backup. It relies on application consistent recovery points being created properly in the first place, and to meet your recovery goals, you also need to ensure you can meet the required restore performance. In a complex, modern production environment, neither of these are necessarily easy to do without the right approach.

Simplifying this complex problem is another area where AI plays a part in Commvault software. It does this in two stages:

- Commvault software understands your mix of applications, data types, OS, speeds and feeds, network bandwidth and other parameters that affect recovery (and specifically recovery, not just backup). You can then group workloads together by application, department and function, and assign your recovery SLA
- A recovery readiness report is then made available, which will alert you to gaps in your desired outcome
- If your report has red flags, AI built into the Commvault scheduler will look at job types, systems, OS/application types, reliability, average throughput and more, and re-organise the schedule to best meet the recovery demands

Not only does this simplify operations and provide clear, outcome-based reporting, but it can have a significant beneficial impact on productivity and it reduces the risk by improving reliability. Clearly, not all performance deficiencies can be made good by scheduling alone, so it will also make recommendations where collection method, backup type or infrastructure changes need to be made.

## RAPID RECOVERY AND RECOVERY SUPPORT

Unfortunately, good security planning and execution are no guarantee that you won't get hit by a WannaCry or Not Petya style attack. Rapid recovery systems can make all the difference, but even these are not a silver bullet, which is when support from your backup vendor can be invaluable.

"To have seen just how quickly these attacks can bring a company to its knees, was breathtakingly scary." Says Simon Powell, Customer Support Director EMEA, Commvault. "However, when those calls came in Commvault did what we do best, we worked with our customers and became an integral part of their recovery plans."



“We got some customers back up and running in a short amount of time, others not so quickly due to the scale of the outage and infrastructure constraints – some literally had to buy new hardware to recover to. The bottom line though still comes down to planning. If you have the best recovery systems in the industry, but you don’t plan on how to recover in all eventualities, and just as importantly, test that recovery plan, then your business faces truly devastating and lengthy outages.”

## CONCLUSION

One only has to take a casual review of the tech media to see the industry concern about this present and ongoing threat, underpinned by organised crime and rogue states, not to mention the part that western governments play.

There is no 100% guaranteed way to avoid this risk, but there are some lessons that can reduce the risk:

- Practice defence in depth, with overlapping security and ongoing training
- Try to catch threats early – laptop backup can provide additional detection tools
- AI provides useful threat detection and recovery planning
- Plan and test, repeat. And repeat again – imagine you’ve lost everything as a start point
- Keep up-to-date printed copies of server/system diagrams and DR plans
- Ensure you have a backup communications system such as personal 0365 accounts, or other sanctioned external IM, preferably set up in advance
- Even if your business does not use the public cloud for production, consider it as a DR target
- Consider bringing in recovery specialists to assess your plans

Ultimately, this kind of planning will make a real difference when you get attacked; being competent in these areas could also have a positive impact on your cyber insurance.

## ABOUT COMMVAULT

Commvault’s converged data management solution redefines what backup means for the progressive enterprise. With innovative products that include Commvault Complete™ Backup & Recovery; Commvault HyperScale™; Commvault Orchestrate™; and Commvault Activate™, Commvault offers an integrated range of backup and recovery, storage infrastructure, service delivery orchestration and data governance solutions.

► Learn more about protecting your organization from cybersecurity threats with Commvault [ransomware protection solutions](#).

©1999-2018 Commvault Systems, Inc. All rights reserved. Commvault, Commvault and logo, the “C hexagon” logo, Commvault Systems, Commvault HyperScale, ScaleProtect, Commvault OnePass, GridStor, Vault Tracker, IntelliSnap, CommServe, CommCell, APSS, Commvault Edge, Commvault GO, Commvault Advantage, Commvault Complete, Commvault Activate, Commvault Orchestrate, and CommValue are trademarks or registered trademarks of Commvault Systems, Inc. All other third party brands, products, service names, trademarks, or registered service marks are the property of and used to identify the products or services of their respective owners. All specifications are subject to change without notice.



COMMVAULT.COM | 888.746.3849 | GET-INFO@COMMVAULT.COM  
© 2018 COMMVAULT SYSTEMS, INC. ALL RIGHTS RESERVED.

