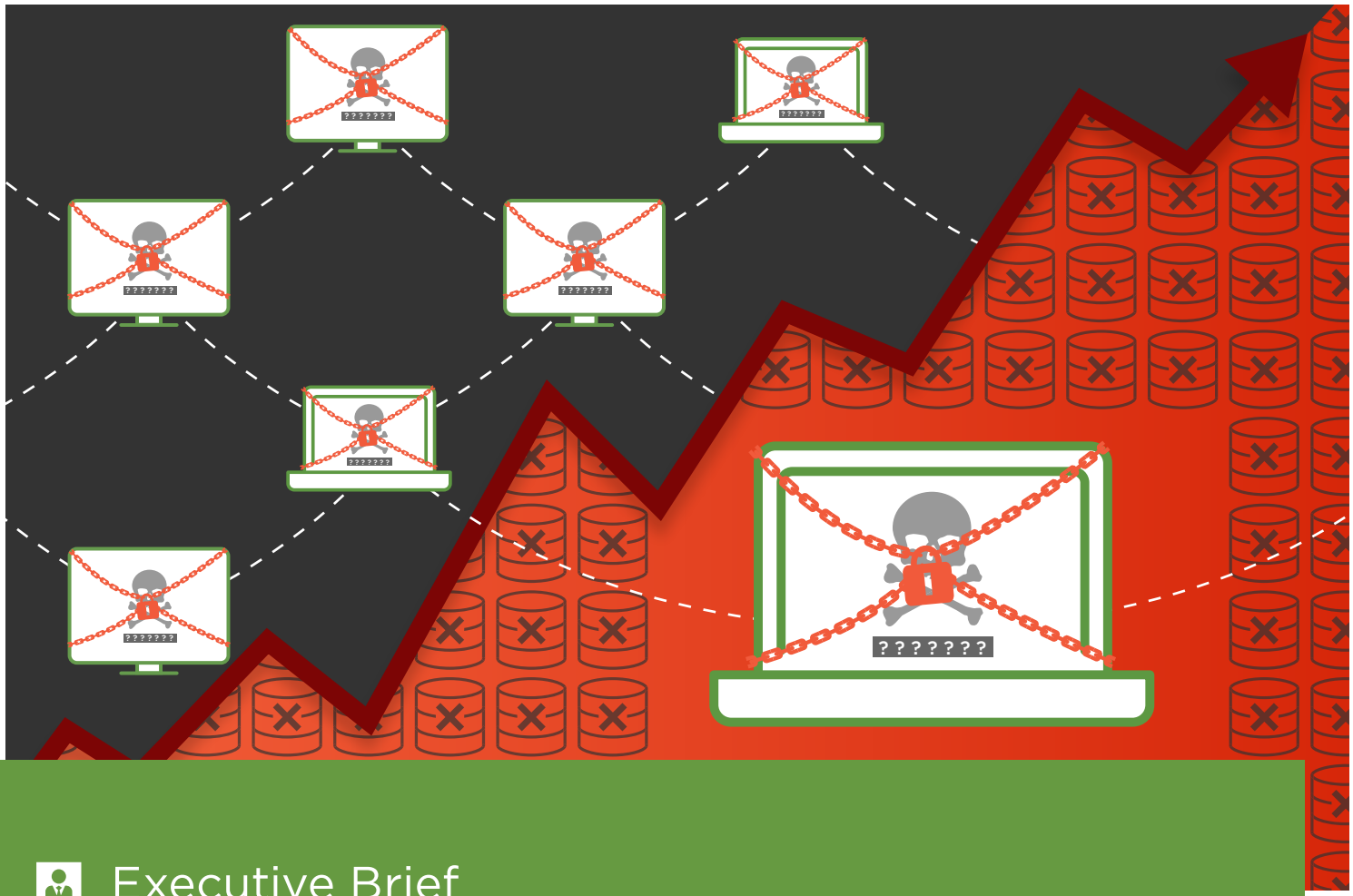
druva



Executive Brief

DRUVA ANNUAL RANSOMWARE REPORT

2017 Survey

Q118-CON-10765

Executive Summary

Nearly every day, there's another story about a ransomware attack in the news. The U.S. Department of Justice reports[1] that an average of 4,000 daily ransomware attacks have been taking place since January 1, 2016. Ransomware has become a sizable international business, and it's now estimated that the global cost for organizations will reach $5 billion by the end of 2017, up 400% from 2016 estimates. The average ransom requested has risen to $2,500,[2] but this number pales in comparison to the hours of lost productivity that businesses suffer and the resources spent trying to recover the data, as well as the time and effort needed to determine the extent of the breach and ensure that the damage has been contained. When you consider the fact that these costs are compounded by the immeasurable consequences of critical data that may ultimately be irrecoverable, it becomes clear that the potential harm inflicted on an organization by a ransomware attack can be extremely severe. With ransomware attacks on the rise, organizations of all sizes have found themselves vulnerable and struggling to reduce risk and respond to an attack.

Against this backdrop, Druva conducted its annual ransomware survey to better understand what impact ransomware has had on organizations, how they have responded to breaches, and what their outlook is regarding the future of these types of malware attacks. This year's survey was completed by 832 IT professionals within multiple industries across the globe in May and June of 2017. We've highlighted our findings in this report.

"Ransomware is on the rise, and backup remains the best protection against data loss. As a fail-safe, organizations should implement enterprise endpoint backup for laptops/workstations, and set recovery point objectives (RPOs) for each server deemed to be at greater risk to ransomware according to organizational requirements based on data loss time frame acceptable to the organization."

–Gartner, Magic Quadrant for Data Center Backup and Recovery Software

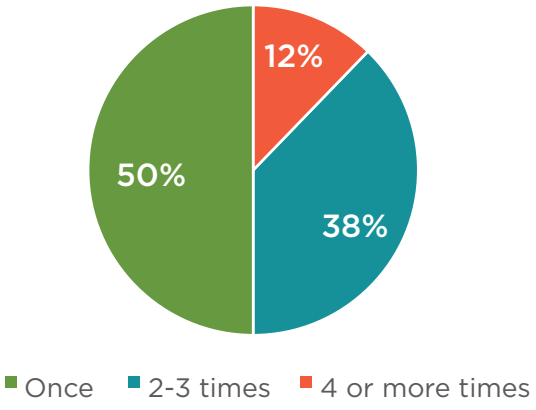
[1] *How to Protect Your Network from Ransomware*, U.S. Department of Justice, 2017.

[2] *The Rise of Ransomware*, Ponemon Institute LLC, January 2017.

Survey Results

Ransomware Isn't One and Done

A ransomware attack can crush organizations that haven't put the proper protections in place. And unfortunately, recovering from a ransomware attack doesn't mean that you are somehow immune going forward. Survey respondents indicated that ransomware is an ongoing threat, with 50% of organizations reporting multiple attacks.



50%

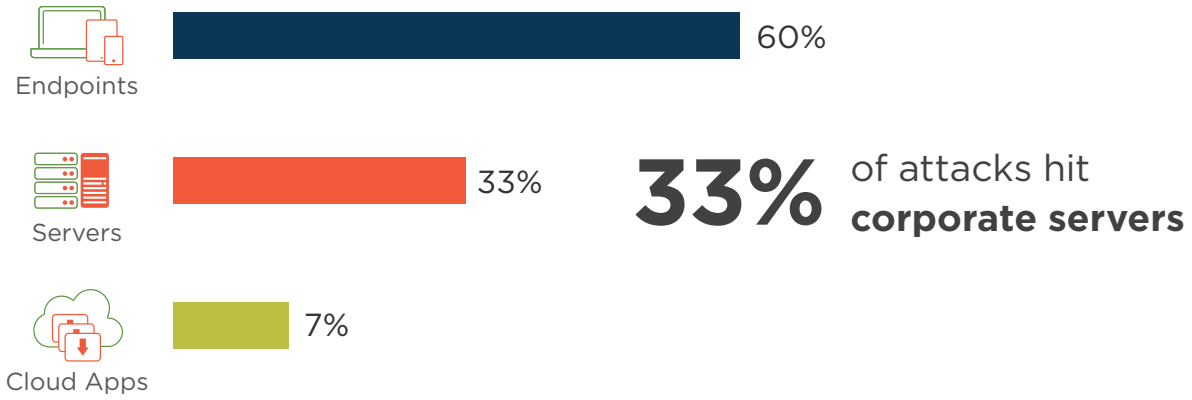
of organizations have been attacked **multiple times**

For organizations struggling to return to business as normal after an attack, repeated attacks can take an even greater toll. The owner of a Michigan radio station[3] reports spending a week recovering from an attack—only to get hit by another attack just one day after business had returned to normal. For organizations that are formulating a ransomware defense strategy, the ability to recover is only one component that needs to be considered. The speed at which that recovery happens as well as all the steps necessary to outline responsibilities and timelines must be included in a ransomware response plan. However, even with a comprehensive plan, every attack will bring some degree of downtime, and companies must be able to minimize this downtime in order to reduce the overall impact on their business.

Not Just an Endpoint Problem

Much of the focus within organizations has been the vulnerabilities that result from employees' lack of understanding and good computing habits. Although the majority of ransomware attacks have succeeded by exploiting security holes left by operational policies that were either inadequate or ignored, allowing malware to infect laptops and other end-user devices, the risk of ransomware attacks against servers is very significant and should be an equally significant part of the conversation. Survey respondents report that 33% of ransomware attacks within their organizations involved servers.

[3] "Tiny Michigan radio station hacked with 'ransomware'—twice in two weeks," *CBC Radio-Canada*, January 20, 2015.



Recent news has highlighted risks that ransomware attacks pose to corporate server environments. South Korean web hosting company Nayana recently found that 153 of their Linux servers had been infected with a ransomware variant called Erebus. The WannaCry attack that affected 200,000 users in 150 countries exploited a known vulnerability in various operating systems, including Microsoft Windows Server 2003. Another variant, called Samsam, specifically attacks a vulnerability in the Red Hat JBoss software. In each of these instances, the respective software vendors were aware of the vulnerabilities and had built patches to address them. However, if organizations are not taking the necessary steps to patch their servers on a regular basis in order to keep them up to date, malware attacks will continue to target these known points of vulnerability. Establishing good system administrative policies and practices is a crucial first step in reducing the overall ransomware risk to organizations.

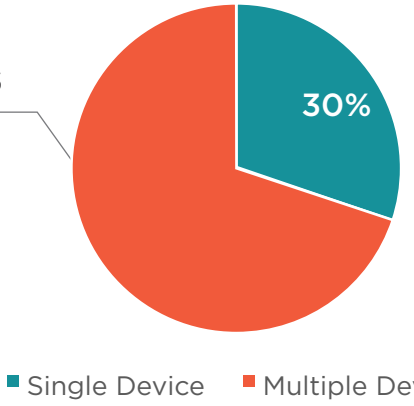
Impact Linked to Speed and Spread

Once ransomware has found an entry point to an organization via employee devices, servers, or cloud applications, it can spread quickly. One infected device may sync to a shared file server or cloud application, spreading malware to the rest of the organization through all the other devices that are connected to that share. Survey respondents reported that 70% of the ransomware attacks within their organizations affected multiple devices.

A recent ransomware attack at University College London[4] was believed to have started due to an employee falling prey to a phishing attempt. The malware spread for five hours before getting reported to IT, at which point it had already compromised the university's network and share drives.

[4] "University College London hit by ransomware attack," *The Guardian,* June 2017.

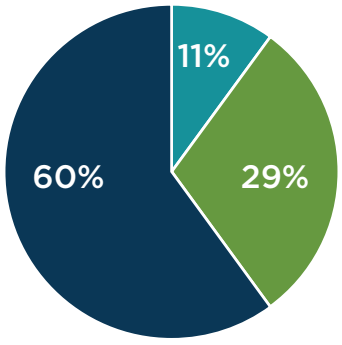
70% of attacks hit **multiple devices**



The more time that ransomware has to spread within an organization before it's detected, the more damage it can inflict. It's critical that IT become aware of a potential attack as quickly as possible, yet the survey results indicate many attacks are not detected immediately. About 40% of the time, more than 2 hours passed before IT became aware of the issue.

Because ransomware often gets into an organization through the ill-advised action of an end user, the infected user may be reluctant to contact IT to notify them of the event immediately. Other types of malware may operate on a time-release basis, meaning that they are within an organization, spreading from device to device, without actually encrypting data or causing other events that might attract the attention of IT.

The speed at which malware spreads combined with the critical time-sensitive need to respond makes it crucial that IT have automated mechanisms in place to detect and be notified of a threat within their network.



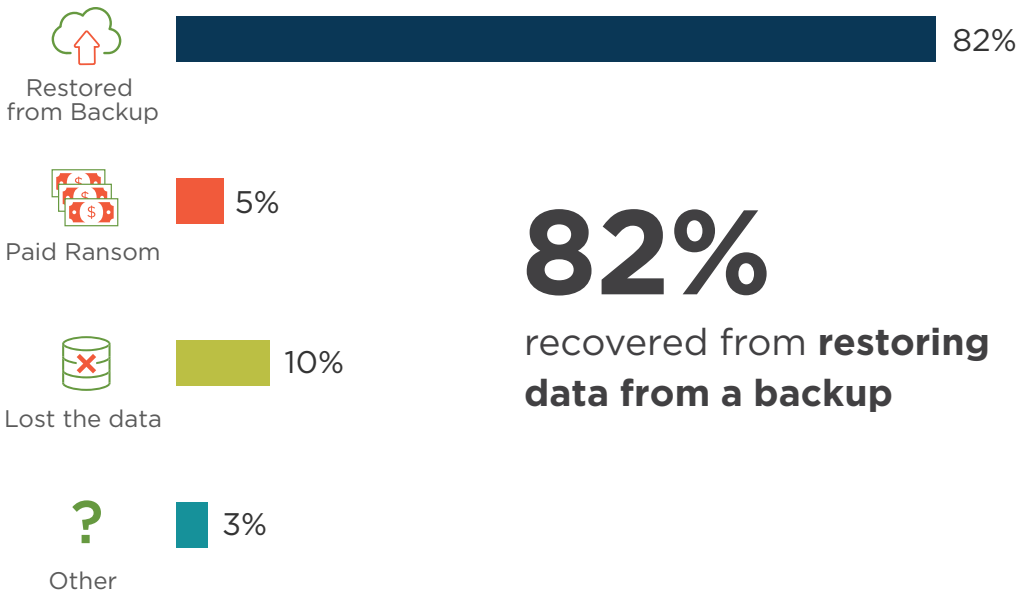
40%

of attacks took **longer than 2 hours** to detect

Backup Is Crucial to Recovery

The actors behind a ransomware attack generally demand some amount of money in return for the decrypted data. However, paying the ransom doesn't guarantee getting the data back. Security firm Kaspersky estimates that 20% of organizations that pay the ransom don't actually get their data back.[5] And in many cases, even when an infected organization paid the ransom, the attackers then demanded a second ransom before agreeing to return the data.

Overwhelmingly the respondents to our survey reported that their organizations had recovered from ransomware attacks—not by paying the ransom, but by relying on their backup data. In fact, 82% of respondents indicated that they used their backups to recover and get the business up and running.



All Organizations Hit Equally

The organizations surveyed were of various sizes, but the data itself was consistent across the entire set. There were no clear differences in the frequency of ransomware attacks or their affect or resolution. Organizations of all sizes are struggling with the same issues and are looking to the same solution to mitigate the damage a ransomware attack can inflict: regular, comprehensive backups.

[5] "To Pay or Not To Pay? Kaspersky Lab Urges More Internet Users to Join the Fight against Ransomware," *AO Kaspersky Lab*, November 2016.

50%

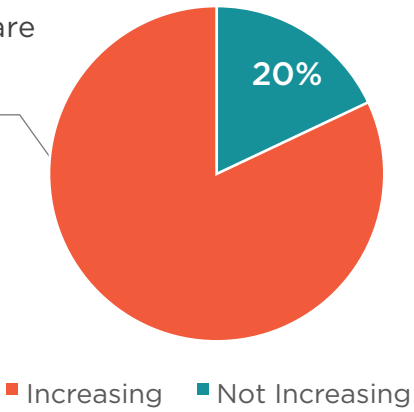
of organizations surveyed had **over 10K employees**

Attacks against critical institutions like hospitals and universities as well as big companies like Sony and Nissan often capture the attention of the media. However, companies of all sizes and across many industries are feeling the impact of these attacks and experiencing the difficulties associated with lost productivity and revenue.

Attacks on the Rise

Unfortunately, it doesn't appear that ransomware attacks are going to subside anytime soon. About 80% of those surveyed believe that attacks against their organization are actually increasing. This means that implementing a comprehensive ransomware recovery plan is something that organizations cannot continue to ignore or postpone. With thousands of attacks occurring each day, organizations can no longer afford to delay protecting themselves.

80% reported that their ransomware incidents **are increasing**



Identify Your Path to Recovery

The survey results indicate that, overwhelmingly, organizations are relying on backup to recover from a ransomware attack. Putting in place a comprehensive plan that covers both structured and unstructured data—wherever it lives—is key to ensuring that organizational data is always secure and available. A scalable and efficient backup plan provides major benefits beyond ransomware, where the data loss can be the result of malware, system failures or user error, along with providing centralized data visibility and governance. Implementing a cloud-based backup solution can provide an additional level of availability and security by leveraging off-site storage in order to reduce the risks of on-prem systems that are often rendered unusable by the very same attacks they were meant to help recover from.

Each organization needs to prepare a detailed plan that fits the specific needs and data landscape of the business. Start with these basic steps when outlining your plan:

1. Don't pay the ransom.
2. Turn all devices off.
3. Disconnect devices from the network.
4. Find the source of the attack.
5. Alert all of your users.
6. Restore from a backup to a new device.
7. Reimage the infected devices.

To learn more about ransomware preparedness and response, visit druva.com/solutions/ransomware/.

About Druva

Druva is the leader in cloud data protection and information management, leveraging the public cloud to offer a single pane of glass to protect, preserve and discover information—dramatically increasing the availability and visibility of business critical information, while reducing the risk, cost and complexity of managing and protecting it.

Druva's award-winning solutions intelligently collect data, and unify backup, disaster recovery, archival and governance capabilities onto a single, optimized data set. As the industry's fastest growing data protection provider, Druva is trusted by over 4,000 global organizations and protects over 25 PB of data. Learn more at www.druva.com and join the conversation at twitter.com/druvainc.

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44 (0) 203-750-9440
APJ: +919886120215
sales@druva.com
www.druva.com