CRIMEWARE REPORT
MARCH 2021

Arete
Incident Response

Post-Mortem Analysis of a Dumpster Fire

For many in the cybersecurity community, the past several months have been a dumpster fire. While doctors and nurses tirelessly cared for pandemic victims in hospitals across the world, our cybersecurity colleagues stood in the digital trenches, slugging it out to defend those same hospitals from ransomware and other nefarious threats. Often against impossible odds, including shoe-string budgets and outdated infrastructures, these teams fought the good fight. And still, the ransomware fire burned on.

Many of us at Arete have been where you are. We understand the precarious, cost-benefit tightrope you walk on a quarterly, if not daily, basis when it comes to making decisions on cybersecurity. We aren't here to sell you snake oil — for one, it doesn't exist. For two, we stand by the fact that our data, experience, and expert insights can help tip the scales in your favor — whether you need help with incident response, negotiation, or restoration.

We've analyzed and tracked definitive data from **more than 1,500** incident response and forensics cases over 12 months to provide unique visibility into the state of ransomware. What's more, we've drawn out nuances from this detailed corpus of trench-fighting, after-action reports that allow us to predict how actors will behave according to circumstance.

Average Ransom Payments

While many variants generated significant payments, Ryuk led the pack [Figure 1.1]. On average, the group negotiated payments of more than US$1 million — success in part due to distribution on the back of TrickBot, one of the most mature and prevalent malware loaders in the cybercrime ecosystem.

Maze (Egregor) came in a close second [Figure 1.1]. Like rats, this digital scourge of a threat group fed off a banquet of available privileged credentials, with average payments nearing the million-dollar mark.

When analyzing payments per month, the largest spike coincided with the COVID-19 summer surge [Figure 1.2]. No doubt, you've seen a dozen graphs that illustrate the same, but let's dive into the nuance.

As the concept of a "network perimeter" began to disappear during this time frame with remote work quickly becoming the new normal, cybersecurity teams who'd previously had a modicum of visibility and control suddenly witnessed their capabilities dissipate.

On average, the Ryuk group negotiated payments of more than US$1 million.

AVERAGE RANSOM PAID BY VARIANT (USD)

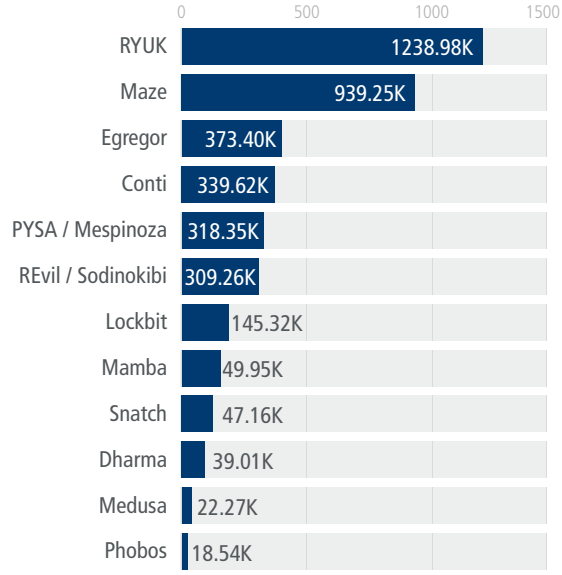


Figure 1.1 Average ransoms paid respective to variant

AVERAGE RANSOM PAID BY MONTH (USD)

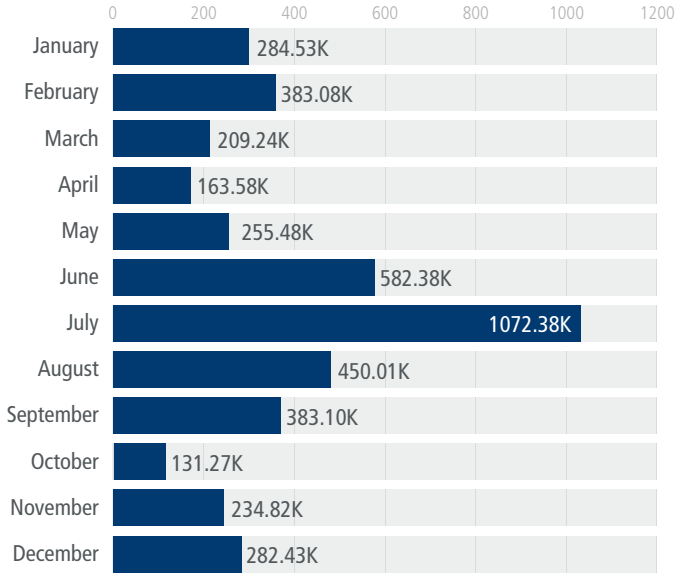


Figure 1.2 Average ransom amounts paid [all variants]

Ransomware Initial Access Vectors

Security is a cost center. Thus, for many security teams, it can be difficult to implement proper segmentation, multifactor authentication (MFA), and defense in depth. When seeking budget and support, they often find themselves unsuccessfully competing against billable business units and overlooked as not crucial to the bottom line.

Still, it comes down to the cost-benefit ratio of implementing security controls versus maintaining an unsecure status quo. As a community faced with exigent circumstances — for example, a global pandemic — organizations have had to make some hard decisions. For the sake of business continuity, many had to expedite remote desktop protocol (RDP) access while watching their perimeters dissolve. Unfortunately, most could not simultaneously execute the deployment of MFA [Figure 2.1] or robust network access controls fast enough to mitigate the new threat surfaces exposed by the hurried RDP access.

Many companies had to expedite RDP access while watching their perimeters dissolve.

Now, let's introduce a growing trend in living-off-the-land tactics, whereby cybercriminals try to hide their malicious activity in legitimate processes, such as a "trusted" SolarWinds software update. Considering the increased use of privileged credentials, provided as a mere consequence to near unfettered remote access, it's not hard to see [Figure 2.2] how managing a combustible, crumbling network infrastructure can ignite into a roaring inferno.

MFA BEING USED?

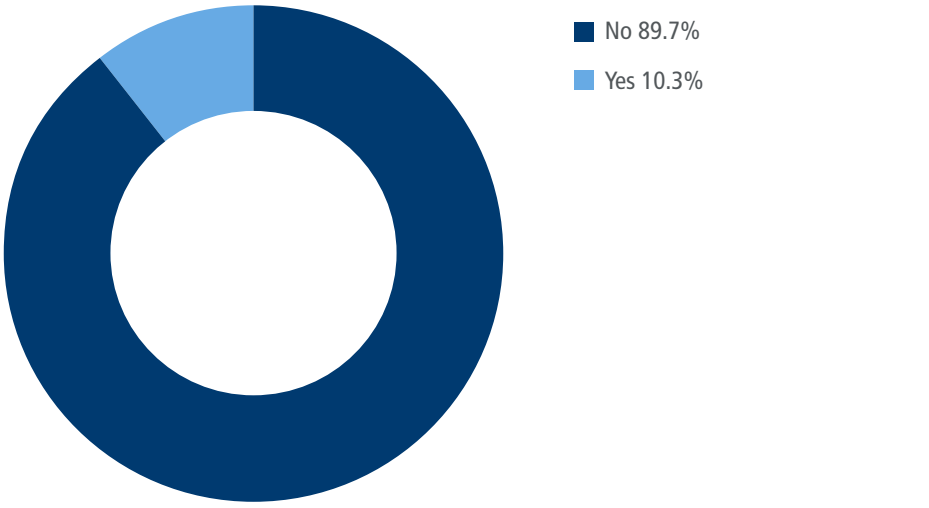


Figure 2.1 MFA use relative to successful intrusion and ransomware deployment

METHOD OF INTRUSION

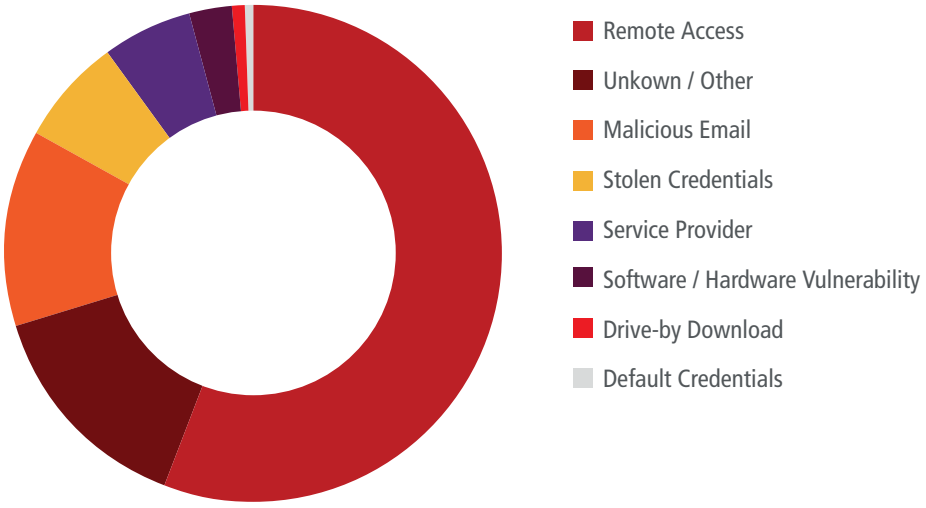


Figure 2.2 Method of intrusion relative to successful ransomware deployment

Data Exfiltration Rates

Though data exfiltration is a trend set by the mature and highly evolved proprietors and operators — Ryuk/Conti, Maze/Egregor, REvil/Sodinokibi, with outliers quickly following [Figure 3] — it is not one occurring across the board for the variety of actors we track.

What many people aren't looking at are the less-robust operators that follow. The ones with poor-quality payloads, erratic communication behavior, or those who easily hijack the work of others — for example, the intellectual property of the bigger players.

These budding cybercriminals — the baby snakes of the ransomware ecosystem — can almost be more dangerous, with their non-functional decryptors and fickle attitudes. In fact, there is almost a greater chance of recovery in the event of exfiltration when dealing with "organized crime."

Like any business, the heavy-hitting "organized" operators have a reputation to uphold; it's to their advantage to make good on their word and provide working decryptors once paid.

459K

Average Ransom Paid in 2020 with Data Exfil

259K

Average Ransom Paid in 2020 with NO Data Exfil

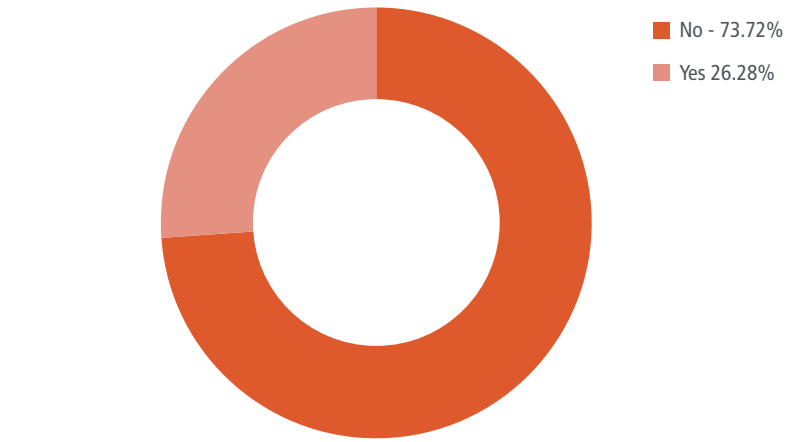


Figure 3 Data exfiltration relative to successful ransomware deployments

Ransomware Impact by Sector and Organizational Size

Cybercriminals are opportunists — and to them, size is relative.

While Ryuk and REvil pursued larger victims for larger gains, they couldn't resist going after smaller organizations, too. Like a forest fire, they were keen to burn whatever dry kindling lay in their path.

REvil, which likely originated from GandGrab ransomware or like platforms, seemed to gain momentum from broader marketplace adoptions in earlier stages. Thus, we're likely to also see a broad variety of cybercriminal targeting at play with more mature ransomware operations due to the brand-following at earlier stages in their cybercriminal life cycle.

INDUSTRIES TARGETED BY RANSOMWARE

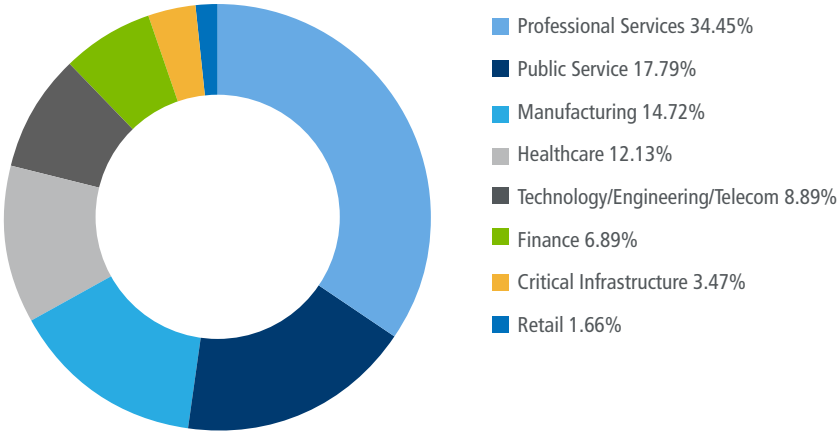
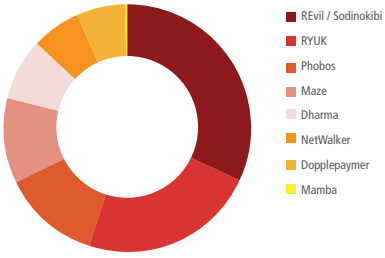
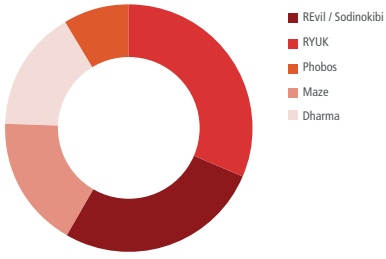


Figure 4.1 Overall impact relative to sector [all variants]

PROFESSIONAL SERVICES VARIANTS OBSERVED



PUBLIC SERVICES VARIANTS OBSERVED



MANUFACTURING VARIANTS OBSERVED

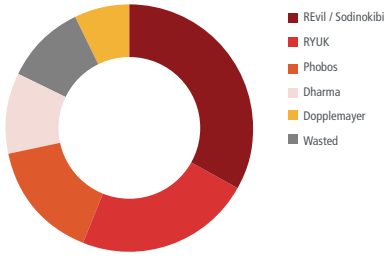


Figure 4.2 Impact to the most impacted sectors relative to ransomware type

Average Time to Recovery

On average, there's negligible disparity on recovery time between small and large businesses. However, there's a noticeable recovery lag with organizations that depend on service providers. Naturally, the mechanics that contribute to recovery are likely out of control scope for impacted clients [Figure 5.1]. As we've seen with past notable instances, service providers also contribute to the threat surface related to the risk of compromised remote access.

Because service providers often require privileged access into client environments to deliver effective service, they have become a popular attack vector for threat actors.

Conversely, compromised accounts are often simpler and faster to remediate than software vulnerabilities. It's relatively straightforward to requisition accounts and credential resets [Figure 5.1]. It's often difficult to have accurate visibility into device inventory and patch status for the same reasons it's difficult to properly segment environments. Security can fall second to the agile and dynamic pace of business needs and consequently, security teams can also struggle to keep pace.

A key (pun intended) contributing factor to recovery lag is receiving reliable decryption keys from a cybercriminal after payment. In fact, reliability can vary considerably among actors, especially given affiliate mechanics of the Ransomware-as-a-Service (RaaS) model [Figure 5.2]. Depending upon agreements with their platform proprietors, affiliates most often operate as middlemen and must relay payments and keys. For most ransomware events, this back-and-forth accounts for the bulk of recovery time.

AVERAGE BUSINESS DOWNTIME BY VULNERABILITY (DAYS)

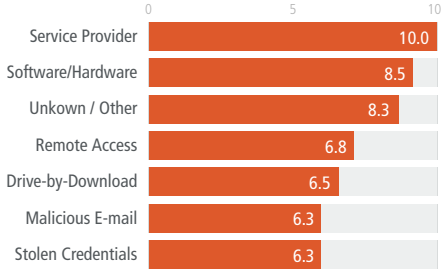


Figure 5.1 Downtime relative to exposure, which led to successful ransomware deployment

AVERAGE BUSINESS DOWNTIME BY THREAT ACTOR RESPONSE TIME

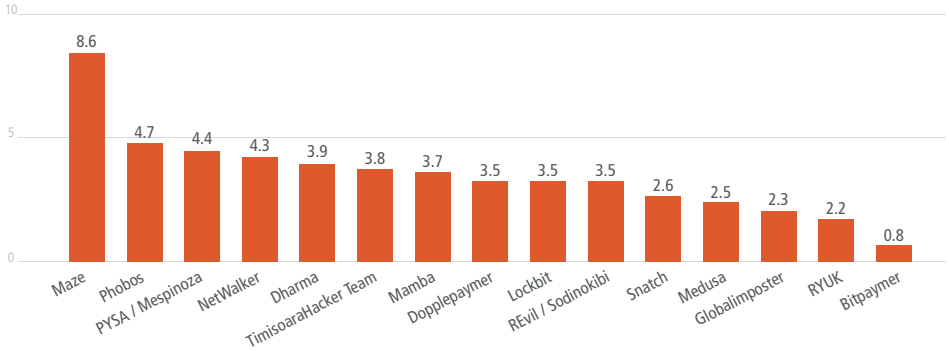


Figure 5.2 Downtime in days relative to response time of threat actors [key retrieval/relative to variants]

AVERAGE BUSINESS DOWNTIME BY INDUSTRY (DAYS)

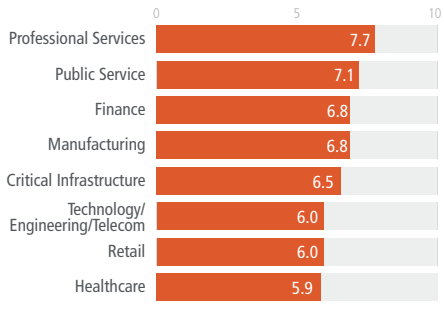


Figure 5.3 Downtime by industry

Backups — An Excellent Strategy If Well-Executed

Here's the unfettered truth on backups. They're great if you're methodical, consistent, and give proper forethought to their protection [Figure 6].

Proper segmentation of networked backups requires strategic planning and attention to detail, often at the expense of competing business initiatives and time spent by capable internal or external human resources for implementation and maintenance. The most resolute and secure backups also require air-gapping and consistency with physical updates. Unfortunately, the resources required to balance this effort may become cost-ineffective depending on budget allocations.

In short, many organizations find it difficult to achieve or maintain effective backups.

Proper segmentation of networked backups requires strategic planning and attention to detail.

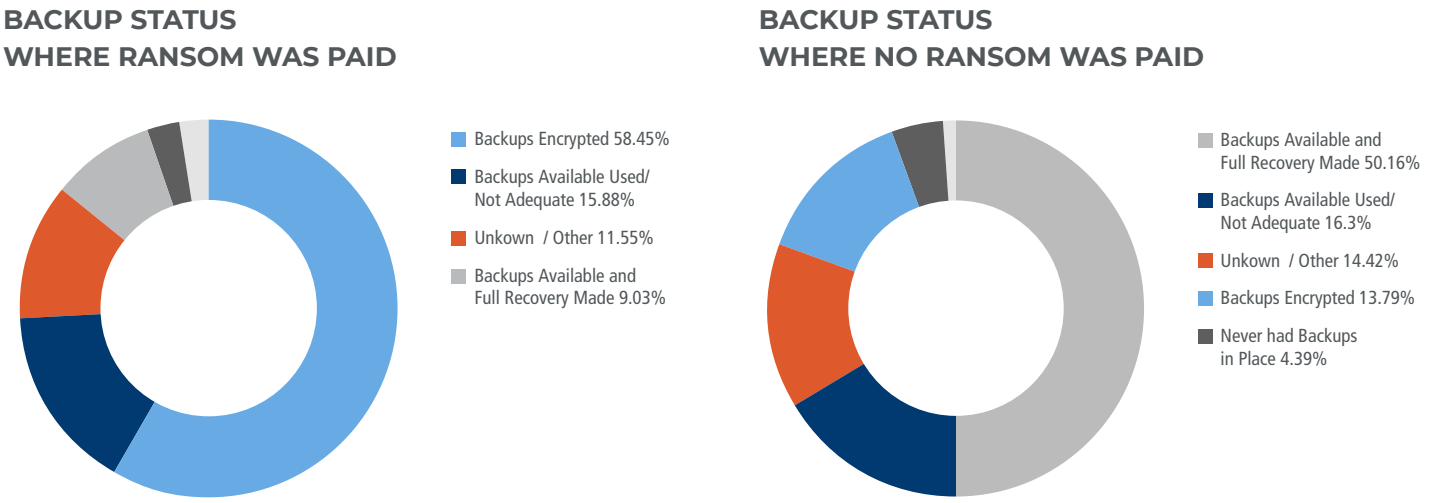


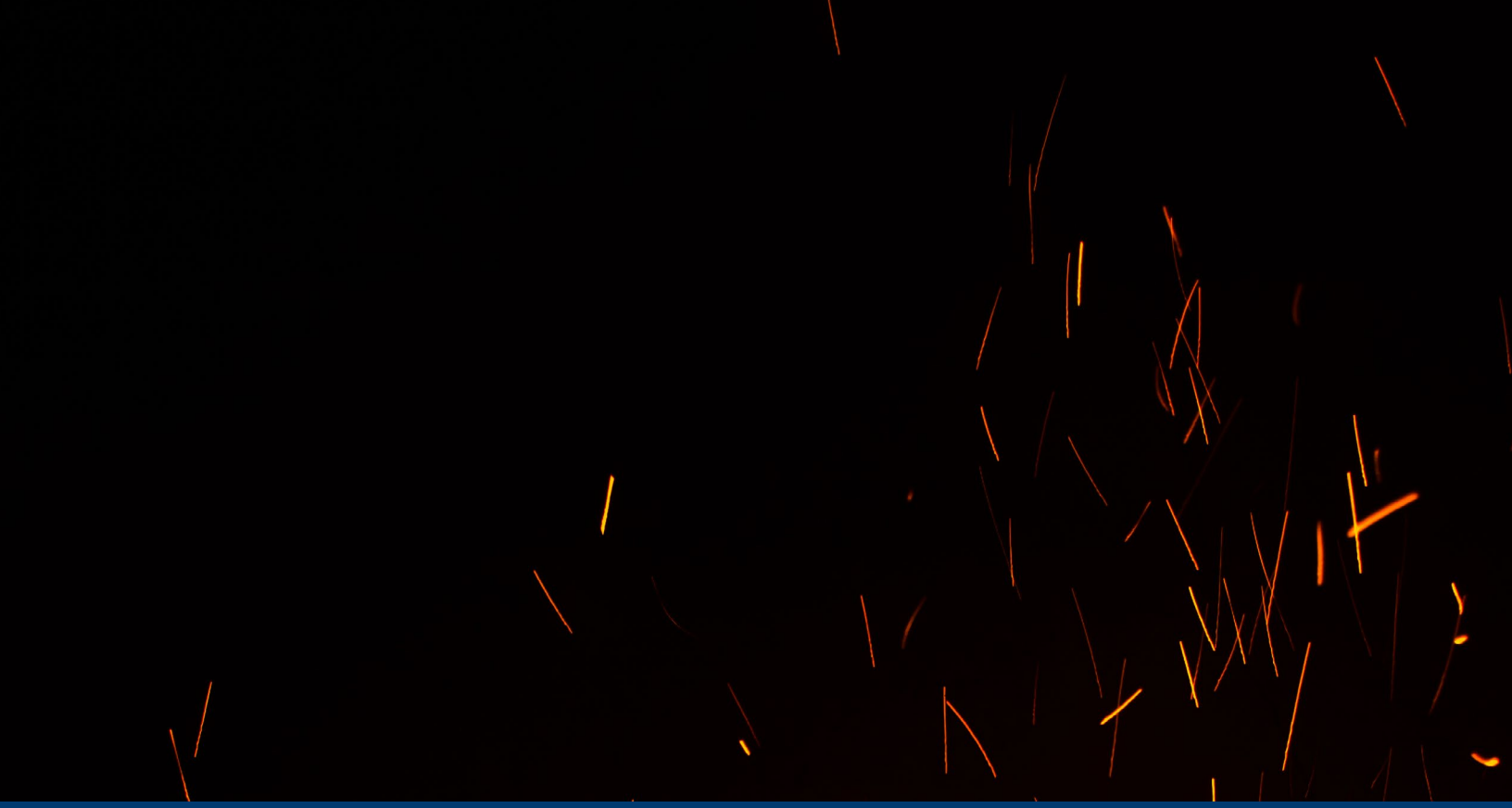
Figure 6 Backup integrity played significant factor in the decision to pay – or not to pay – for all events

We Didn't Start the Fire — But We Don't Have to Be Victims of Circumstance

The state of cybersecurity was a hot mess before the pandemic and created "ripe" opportunities for the cybercriminal economies to grow from the festering rot. Someone is always going to take advantage of a stinky situation, and the bad guys did. Unfortunately, many organizations weren't prepared to adequately defend themselves and they paid dearly — in ransoms, lost business, damaged reputations, and even, closings.

If security is important to you, you'll find a way to get it done.

You'll make the cost-benefit decision that's right for you. And perhaps you'll engage with those who sort beasts for a living and know how to execute a simple, but effective security strategy — before the flames are lapping at your door.



Arete
Incident Response

Cyber Emergency Helpline 866 210 0955
Phone 646 907 9767

New Engagements
Arete911@AreteIR.com

www.areteir.com