# ANNUAL GLOBAL IT SECURITY SURVEY 2022

## securing a permanent remote workforce

APRICORN

# Apricorn 2022 Global IT Security Survey.

## *Cyber resilience and remote work policies at forefront of security concerns*

As the world was plunged into a blended chaos of lockdown and uncertainty at the onset of the pandemic, IT security teams were forced to respond at speed, creating temporary contingency plans to ensure that employees could continue working remotely, despite the inadequate security measures in place.

Two years on, many organizations have elected to keep remote and hybrid work protocols in place. Indeed, data from our 2022 survey shows that remote working remains a standard practice in more than four in five organizations. Yet this new normal presents a new challenge facing IT security professionals.

Having had to deploy remote programs under massive time constraints in 2020 and 2021, security teams are now faced with quickly trying to fix the gaping holes that these rushed deployments created.

With remote and hybrid working here to stay, cybercriminals are becoming bolder in their efforts to capitalize on new exposures. Indeed, one report shows that the average ransom demand was $2.2 million in 2021 – a 144% increase from the average demand of $900,000 in 2020.[1]

Promisingly, it appears many organizations are going back to address new vulnerabilities. According to our respondents, more than half of security teams have since updated data security policies and processes that they first put in place two years ago.

However, despite the positives, it is also clear critical security policies are not being enforced and/or followed, and cyber resilience remains a challenge.

Our findings show that one in four employees are recognizing policies but not adhering to them. Meanwhile, IT departments lack the tools to monitor and enforce policies effectively, while their desire for stronger security policies such as the mandated encryption of USB storage devices are not being met.

Given the escalation of security threats, time is of the essence in addressing these issues.

Without question, cyber-resiliency – the availability to access and resuscitate data in the event of a ransomware or other cybersecurity attack – needs to be an organizational priority. Companies that haven't yet been hit by a cyber attack are lucky. Now is the time to put policies and strategies in place to both protect their data, and recover it fully should it be compromised/ransomed.

## Key findings include:

- Security and compliance have risen up the agenda of four in five companies as a result of the shift in working environments. Additionally, the same proportion have gone back and reviewed the security policies and practices that were initially implemented in a rush to accommodate a quick shift to remote working.

- Eighty percent of organizations have developed remote working policies, with 56% reinvesting in reinforcing employee education. However, one in four firms state that despite having such protocols in place, employees are not adhering to them.

- Of the IT security professionals surveyed, 72% say employees do not consider themselves to be a target that attackers would exploit to access company data, driven by perceptions that they are either too small a target and/or adequately protected.

- While 82% agree that the use of encryption of USB devices should be required for their organization, only 34% have put a policy in place to mandate encrypted USB storage devices for protecting data on the move.

- Three in five companies do not back up their data or devices in advance of working remotely, while only one in five follow backup best practices such as the 3-2-1 storage strategy and backing up in real-time.

- More than one in four (26%) view the cloud as too risky for data backup, but only one in three back up to both the cloud and encrypted hardware storage devices.

*"For many companies, the hybrid workforce is here to stay, regardless of pandemic status. Outside of the firewall, IT security professionals focus on securing that remote workforce with ever-evolving policies and ongoing aggressive employee education and training."*

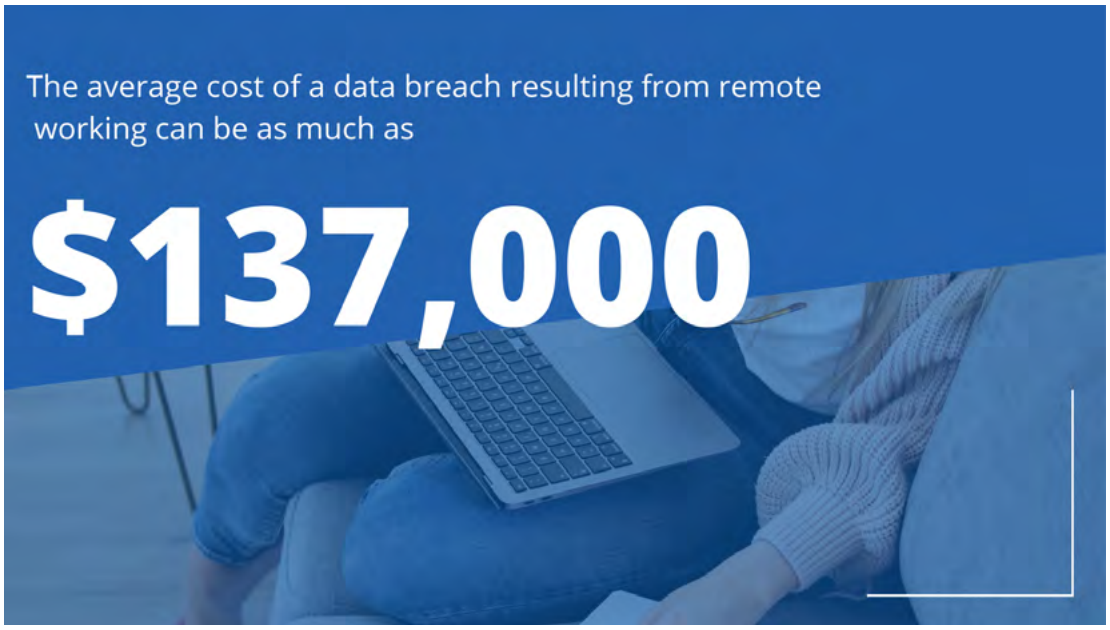
***Kurt Markley*** -- Managing Director, Apricorn USA

## Security and Compliance are Growing Priorities


The rapid transition to remote working dramatically increased risk for many organizations. PwC acknowledges that many companies took a "connectivity first" approach in their initial response to national lockdowns and social distancing mandates.

> *"Those policies exist to protect the business from bad actors (internal and external). The reason risk reviews take time is most companies have very complex IT environments. Many employees now use remote desktops and unapproved file sharing and applications ("shadow IT"). Consequently, many companies can't answer a basic question: "which assets can my remote users see and access?" Security breaches could be occurring right now and remain undiscovered for months."*
>
> PwC: "COVID-19: Making remote work productive and secure"[2]

For cybercriminals, remote work presents significant opportunities. According to Deloitte, 47% of individuals fall for a phishing scam while working at home, while the average cost of a data breach resulting from remote working can be as much as $137,000.[3]




As a result, many organizations are increasingly recognizing the need to develop secure remote working models in order to curb potential attacks and save time, money and significant headaches in the long run.

Our survey shows that IT security pros and companies are proactively attempting to instill more effective and secure remote and hybrid working models, with more than half having updated security policies and processes since remote working initially became normalized.

More than half (57%) are testing that their remote access capabilities are tested and secure, 43% are reviewing data security roles and responsibilities, and 37% are focusing more readily on resolving outstanding regulatory and compliance issues.

> *"60 percent of small and midsize businesses that are hacked go out of business within six months."*
>
> The US National Cyber Security Alliance [4]

## Ahead of the Game?


The evidence is clear. The vast majority of organizations are now actively addressing security concerns in the new normal to eliminate potential vulnerabilities, mitigate threats and enhance their security posture. And such efforts are seemingly paying dividends.

76% of respondents are concerned about connecting to other networks or corporate devices when they work remotely, for example.

On the surface, it might appear that IT security professionals are ahead of the game with regard to securing remote workers and their devices. However, despite the positives, we can equally see that there are still significant holes that need to be addressed if organizations – and their data – are to be considered truly resilient.

While 80% have gone back to deal with rushed remote working security policies and practices, a full 20% of organizations that moved quickly to put a remote or hybrid work environment in place during the pandemic have not gone back to address newly implemented security policies or practices . Indeed, some may have been confident with the changes that were made from the outset, yet in such a volatile environment the consistent scrutinization of security policies has never been more important.

Furthermore, while respondents consider certain security scenarios, they aren't covering the full spectrum. More than half of respondents are not concerned about sharing devices with co-workers, friends or family members (61%), backing up their data or devices before working remotely (69%), or accessing corporate data or documents from personal devices (52%).

Specifically, our 2022 survey has shone a spotlight on three core issues facing IT security teams in the current environment – the need for encryption, the importance of cyber resiliency and backups, and employee-centric vulnerabilities.

## Encryption Must be Mandated

While 82% agree that the use of encryption of USB devices should be required for their organization,


A sure-fire way to help mitigate the possibility of security breaches is through the implementation of hardware encryption.

Encryption and endpoint control can ensure data remains secure, reducing the risks that come with remote working, while end-to-end encryption can also be deployed to ensure that third parties cannot decipher a document, email or message without the encryption key.

> *"Organizations increasingly need to improve their data security strategy, and may be required to meet data protection regulations as they scale in the cloud. The correct implementation of encryption methods can provide an additional layer of protection above foundational access control mechanisms providing a mitigation if your primary access control policies fail."*
>
> AWS blog [5]

When authentication and encryption take place within the device itself, passwords and key data are never shared with the host computer. This makes hardware encryption well suited to highly regulated sectors such as defense, government, finance and healthcare.

Hardware encryption, such as hardware-encrypted USB storage devices, is particularly secure. Devices that are software-free eliminates the risk of keylogging and doesn't restrict usage to specific operating systems.

Encrypted USB storage is a simple, easily accessible way to boost data and information security across a more mobile organization, the convenience of solid-state based USB drives, sticks or keys making them incredibly popular with users.


Given the widespread adoption of hybrid working models, we asked our survey respondents what external storage policies and procedures have been put in place regarding protecting corporate data on the move. And while four in five organizations do permit external storage options, little more than a third have corporate mandated encrypted USB storage devices.

Further, the survey also suggests that more than one in three of employees (37%) with a lost or stolen USB storage device wouldn't notify the appropriate authorities of the incident.

If organizations are trusting their employees with sensitive corporate data, they must also equip them with the tools, knowledge and education to keep that data secure.

Interestingly, IBM's Cost of a Data Breach Report previously pointed to the extensive use of encryption as having the greatest impact in reducing breach costs – ahead of data loss prevention, threat intelligence sharing and integrating security in the software development process (DevSecOps).[6]

Encryption is therefore critical. As well as helping to reduce the financial impact of a breach, it is a means of demonstrating your trustworthiness and reliability in the realm of data protection, providing your own data-anxious customers with complete peace of mind.

# Backups are Needed for Effective Cyber Resilience and Ransomware Readiness


Organizations should always expect a ransomware attack to be just around the corner, and in turn have the protocols in place to recover quickly and effectively should they need to. Failure to do so can be costly:

IBM reveals that the global average toll of a data breach is now $4.24 million per incident – the highest amount in the 17-year history of its Cost of Data Breach report.[7]

Sophos estimates that the average cost to recover from a ransomware attack is $1.85 million, this figure owed to downtime, people time, device costs, network costs and other lost opportunities alongside ransomware payments themselves.[8]

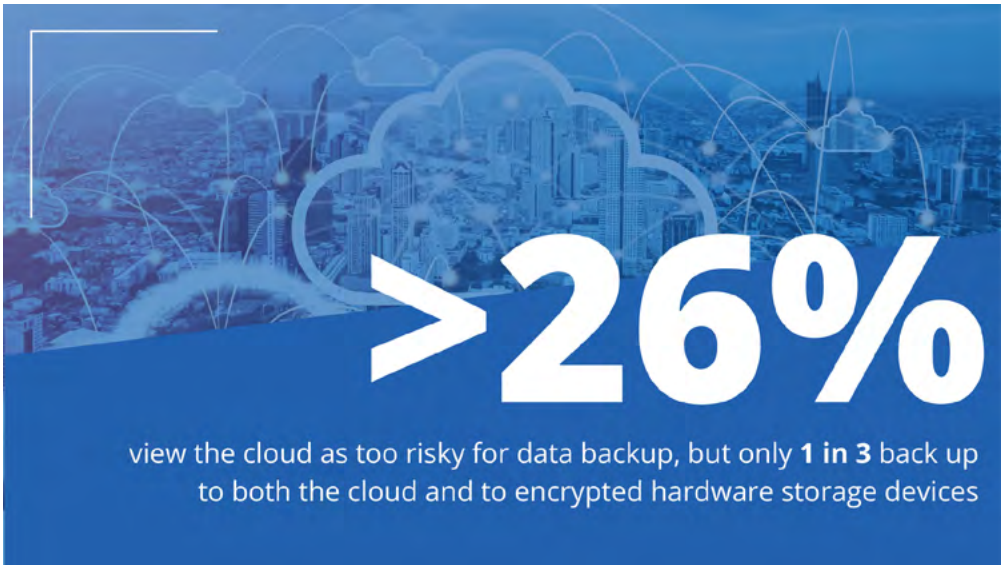
Coveware reported that the average downtime for businesses as a result of a ransomware attack was 20 days in Q4 2021.[9]

Such financial penalties can cripple even the most financially savvy companies. To prevent costs and operational downtime from escalating in such a manner, companies need a rapid response plan that will enable them to get back online and operational at speed – a strategy that needs to begin with backup best practices.

Apricorn recently conducted a Twitter poll exploring device data and backup processes. When asked to be honest with their admissions regarding when they last backed up the important files and documents on their home computer, 57% responded indicated that they do not know or that they may never back up their content.[10]

Meanwhile, World Backup Day reveals that 21% of people have never made a backup.[11]

Businesses today depend heavily on cloud storage as a convenient, fast and secure way to back up critical information off site. This has its merits, but relying on any single solution leaves organizations vulnerable to a data breach or loss.




Companies instead must work to develop a multi-layered backup strategy that incorporates the use of a physical backup located off-site to complement the use of the cloud. In doing so, they can retain an element of control in their backups, ensuring they can always recover and restore from a clean, protected data set.

Here, the 3-2-1 rule is an easy guiding principle in developing a resilient backup strategy. This stipulates that you need a minimum of three copies of data (one primary copy, and two backups) in at least two different locations, and with one dataset stored offsite.

Ransomware attackers will typically target backups to stop companies from restoring the data that they exfiltrate and encrypt, forcing them to pay their ransom. By both geographically distributing backups as well as creating readily maintained offline and online versions, these threats are mitigated.

Currently less than one in five organizations follow the 3-2-1 rule. Yet it is vital that online and offline storage go hand in hand.


Of course, the benefits of creating backups are significantly diminished if you can't leverage them effectively in critical moments.

A playbook should therefore be developed that outlines the process of performing data backup – who is involved, which programs and products need to be used, and the location of the backups. It should also include the procedure for testing, reviewing and updating the process.

Should any staff be absent in the event of an attack, or critical cogs in the recovery chain leave the company, the firm will still retain a step-by-step guide enabling them to respond effectively.

## Employee Education


Alongside policy and resilience, education is vital.

One of the most common ways in which data breaches occur is via physical actions (think a government employee leaving a classified laptop on a train accidentally). Indeed, World Backup Day highlights that 113 phones are lost or stolen every minute, while 29% of data loss cases are caused by accident.[11]

Human error isn't just physical, however. It can equally involve sensitive information being sent to the wrong person via email, or employees falling prey to social engineering attacks such as phishing.

This is a major challenge given the fact that the human is often targeted as the key gateway used by attackers. Alarmingly, IBM reports that 19 in every 20 breaches could have been avoided if human error hadn't been involved.

> *"What is fascinating – and disheartening – is that over 95 percent of all incidents investigated recognize "human error" as a contributing factor"*
>
> IBM Cyber Security Intelligence Index Report [12]

Human error is to some extent unavoidable, no matter how extensively employees are trained. However, what is worrying is the fact that one quarter of respondents noted that the strict remote work policies they put in place are not being adhered to by employees, despite 82% of firms continually reinforcing them.

When remote policies are not followed it's usually due to employees not prioritizing security practices despite being informed about them (51%), or because they are using personal devices for working purposes (40%).


Much work is still required to ensure employees do adhere to all important security best practices and protocols.

The saying that a chain is only as strong as its weakest link rings true. Given that the survey also suggests that 72% of employees believe they are either adequately protected or too small to be a target, a widespread mindset shift is needed to dramatically enhance security protocols and practices.

Not only do employees need to be trained to identify phishing, but they need to take security matters into their own hands, recognizing their actions as hugely impactful on security's overall effectiveness. Data security is not the responsibility of just one person within an organization; every employee plays a part.

Something as simple as having strong passwords can make all the difference. Attackers will still try to access a large number of accounts via password spraying attacks. Through ensuring that you have no weak or common passwords throughout your entire network, you will mitigate this threat.

Organizations should take this a step further and adopt multi-factor authentication (MFA), introducing an additional layer of security. MFA requires your users to identify themselves by more than a username and password, making it a key component of any strong identity and access management policy, directly combating brute force attacks.

> *"The most common initial attack vector, compromised credentials, was responsible for 20% of breaches at an average breach cost of $4.37 million."*
>
> IBM 2021 Cost of a Data Breach Report [7]

# Employee Education (continued)

Most employees perhaps trust their company security policies and procedures too much. Indeed, as hybrid work has been normalized, left employees may have become increasingly complacent or comfortable.

Companies are beginning to respond. Now that hybrid work is a standard practice, more than half (56%) of companies are investing in reinforcing employee education. Yet 100% should be regularly reinforcing education on security.

As threat vectors evolve, staff should remain updated on an ongoing basis, at least annually. Therefore, this 56% represents just the start of what is required on a broader scale.

# Multi-Layered Security is Vital

Given the threat landscape of today, businesses need to make certain that they have an effective backup and cyber resiliency plan so they can respond quickly should a breach occur.

By strengthening capabilities to protect and encrypt data, restore data quickly after an incident, and understand and remediate any cause or causes of an attack, they will be well placed to manage threats that might otherwise have catastrophic impacts.

Mindset is critical. Data protection should never be an afterthought, only adopted because of an incident or as a reactive response to regulatory issues such as GDPR in the UK or Consumer Data Protection Acts across the U.S. To achieve security best practices and mitigate growing risks, it must be placed at the core of business operations.

Just as backup strategies need a layered approach of both offline and cloud-based backups to be covered comprehensively, organizations need a range of blended solutions to be successful.

All enterprises should analyze their data, identify everything that should be protected, understand where it exists and how it is transported, and then ensure that it is encrypted at all stages of its lifecycle.

The risks of failing to cover all bases are clear. Data shows that 37% of organizations were affected by a ransomware attack in 2021, while just 8% of companies typically recover all of their data after paying a ransom.8

Enterprises cannot simply rely on the word of criminals. Instead, they must implement effective backup strategies and response strategies to ensure that data always remains on lockdown.

## About the Survey

The Apricorn 2022 Global IT Security Survey canvassed the perspectives of IT security practitioners worldwide – primarily from countries in North America and Europe. Of the 397 total respondents, 83% have more than five years working in security IT, 45% have 16-20 years working in IT security, 64% either help make the final decision or are the sole decision makers, and more than a third work in organizations with more than 3,000 employees.

Alongside the representatives from large corporations, the survey attracted responses from small business and medium-sized enterprise segments, as well - thus guaranteeing a diversity of perspective.

Respondents were asked about their organizations' security practices and policies around remote working over the past 12 months via question-and-answer options.

The survey, carried out online from March 21 to April 4, 2022, incorporates views from the full spectrum of industry, including company types operating in public and private sector environments. The top five verticals represented are healthcare (14%), IT (14%), Education (14%), Financial Services (10%) and Manufacturing (10%).

## ABOUT APRICORN

Apricorn provides secure storage innovations to the most prominent companies in the categories of finance, healthcare, education, and government throughout North America and EMEA. Apricorn products have become the trusted standard for myriad sadata security strategies worldwide. Founded in 1983, numerous award-winning products and patents have been developed under the Apricorn brand as well as for a number of leading computer manufacturers on an OEM basis.

# References


1. https://unit42.paloaltonetworks.com/2022-ransomware-threat-report-highlights/
   2022 Unit 42 Ransomware Threat Report (Mar 2022)
2. https://www.pwc.com/us/en/library/covid-19/making-remote-work-productive-secure.html
   PwC: "COVID-19: Making remote work productive and secure" (2020)
3. https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html
   Deloitte: "Impact of COVID-19 on Cybersecurity" (2020)
4. https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html
   Statistic from the US National Cyber Security Alliance (2018)
5. https://aws.amazon.com/blogs/security/top-10-security-best-practices-for-securing-backups-in-aws/
   Amazon Web Services Security blog (2022)
6. https://www.ibm.com/downloads/cas/RDEQK07R
   IBM: "Cost of a Data Breach Report" (2019)
7. https://www.ibm.com/uk-en/security/data-breach
   IBM: "Cost of a Data Breach Report" (2021)
8. https://www.sophos.com/en-us/content/state-of-ransomware
   Sophos: "State of Ransomware 2021 Report" (2021)
9. https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts
   Coveware Quarterly Report (Oct 2021)
10. https://apricorn.com/twitter-poll-on-data-backup-policies/
    Apricorn Twitter poll on data backup policies (Oct 2021)
11. https://www.worldbackupday.com/en/
    World Backup Day (2022)
12. https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF
    IBM: "Cyber Security Intelligence Index Report" (2014)