



WHY DATA SECURITY IS REQUIRED FOR MEANINGFUL DIGITAL TRANSFORMATION

 **311%**
was the increase
in the total
amount of
ransoms paid
by victims over
the previous
year.¹

In November 2021, major insurance firm Lloyd's of London (generally known as Lloyd's) made a startling announcement: The insurance and reinsurance market that holds nearly 20% of the globe's cyber insurance market was discouraging its syndicate from taking on new cyber business in 2022.² Just a month later, the firm indicated they will no longer cover cyberattack incidents attributable to nation-states.³ This series of revelations came months after American International Group (AIG) revealed its plans to tighten the terms and conditions of its own cyber insurance policies.⁴ This sudden change in direction was not due to a lack of demand, but for the overwhelming increase in claims.

Just as a devastating hurricane wreaks havoc on property insurance companies, cyber insurance companies are also overwhelmed with claims. According to Fitch Ratings, demand for cyber insurance increased by 28% in 2022.⁵ The reasoning stems from the exponential growth of ransomware attacks over the past 18 months. In fact, the total amount of ransoms paid by victims increased by an astounding 311% over the previous year. Now, couple that with the spiraling costs of remediation, which rose from \$700,000 to more than \$1.85 million in that same period, and you begin to get a clearer picture of the losses absorbed by cyber insurance providers.⁶ Plainly put, cyber insurance is no longer as profitable as it once was in today's diverse threat environment.



GREATER DIGITAL AGILITY ATTRACTS MORE CYBERATTACKS

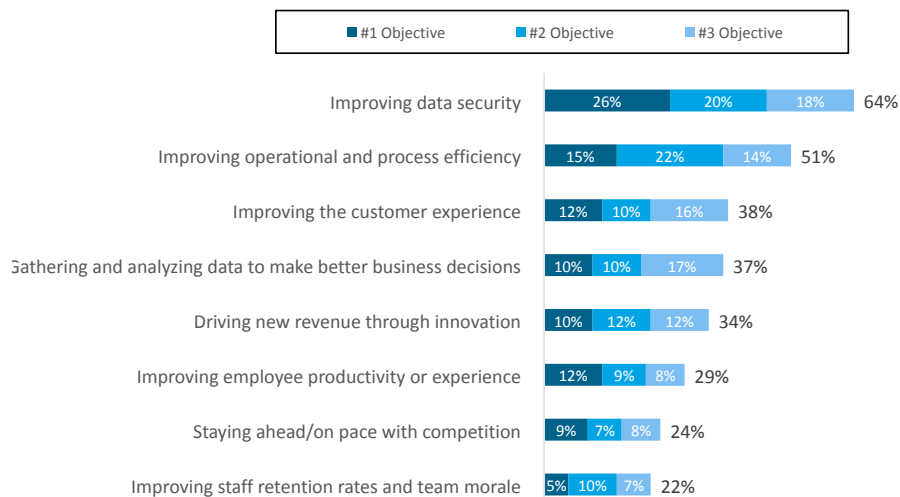
A top reason why companies pursue digital transformation strategies is to attain greater agility, which allows enterprises to better serve their customer base. In fact, 68% of companies identify agility as one of their most important initiatives.⁷ Unfortunately, a digitally connected world also leads to greater opportunity for hackers and threat actors, too. As enterprises are now comprised of vast IT estates with thousands of touchpoints, each one represents a potential vulnerability or attack avenue. Here in North America, ransomware attacks on targeted networks increased by 104% in 2021, per SonicWall’s 2022 Cyber Threat Report. Additionally, governments worldwide witnessed an 1,885% increase while the healthcare industry experienced an increase of 755%.⁸

This story of increasing cyberthreats isn’t limited to just ransomware—there were 1,862 data breaches reported in 2021, an increase of 68% over the previous record set the year before.⁹ Not only has the frequency of breaches risen, so has the cost of recovery. According to the Ponemon Institute, the cost of a single data breach in 2021 was \$4.24 million, a 10% increase over the average cost of \$3.86 million in 2019.¹⁰ Organizations that implemented remote work strategies paid an average of \$107 million higher than the organizations that did not. This was attributed to a lack of technology improvements needed to go remote. Even more alarmingly, organizations that had more than half of its staff working remotely took 58 days longer to identify and contain a breach.¹¹

DATA SECURITY IS THE #1 IT INVESTMENT OBJECTIVE

Whether it is a data breach or ransomware attack, the increased velocity of cyberattacks are a clear reminder that IT leaders cannot digitally transform their organization and ignore digital data security simultaneously. That’s why it should be no surprise that improving data security is a top objective of IT leaders who participated in a recent study. As shown in the chart below, 64% of survey participants ranked improving data security—an increase by almost 40% over 2018.

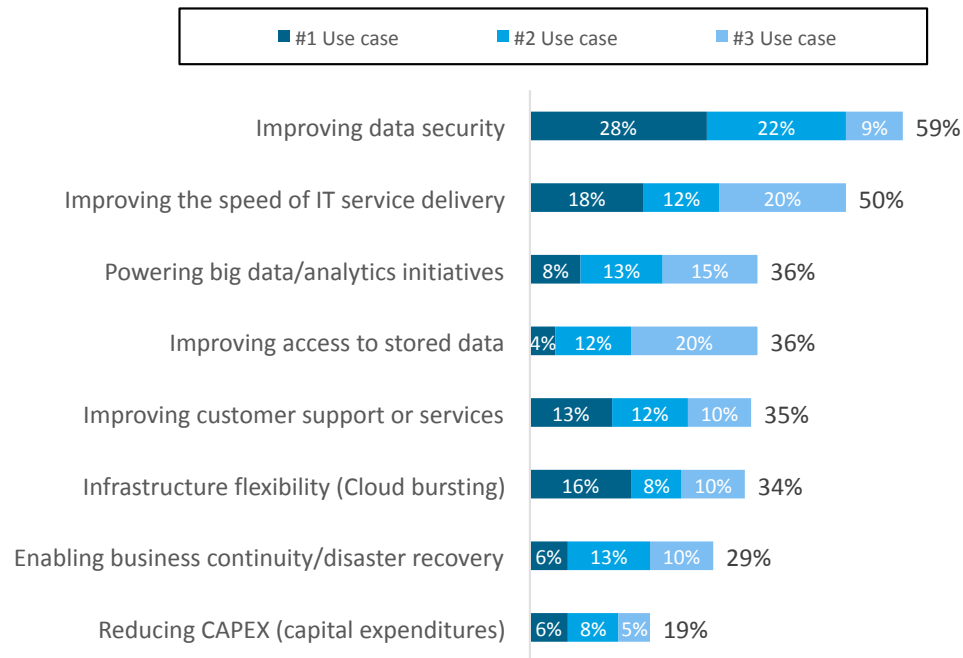
Top IT Investment Objectives - Next 12 Months





Because so many organizations have migrated resources to the cloud, the study also included a focus on cloud utilization. The necessity to improving data security within the cloud was the top driver with 59% citing it as a top three objective.

Top Use Cases for Cloud Technology - Next 12 Months



DEFINING DATA SECURITY

With so many organizations focusing their attention on data security resources, it is important to understand what the term 'data security' really means. Data security is only one piece of the cybersecurity puzzle, and it is sometimes used interchangeably with data protection, which is not the same thing. Additionally, there is the issue of data privacy when it comes to regulatory compliance and litigation. We breakdown these terms below:

- **Data security** refers to the prevention of unauthorized access or use that could result in the compromise, deletion, or corruption of involved data. A large part of data security is about using access control mechanisms to selectively restrict access to only those that are authorized to view and work with the involved data. Another element is the utilization of encryption to prevent an unauthorized party from using the data if breached.
- **Data protection** involves backing up or duplicating data to another location to protect against its loss or corruption due to an accidental deletion, malicious attack, or natural disaster. The ability to restore your data serves as a protectionary measure.



- **Data privacy** refers to the collection, handling, and storage of sensitive data such as personal health information (PHI) and personal identifiable information (PII). It involves regulatory concerns, notification, and consent of use. A common example is the notification a website prompts to users asking for their consent to use tracking cookies.

Data security, protection, and privacy often work in conjunction with one another. For instance, you may implement a multifactor authentication system to properly authenticate users before connecting to a data directory. Should a threat actor seize a privileged account with the required access to encrypt the directory, a backup system can be used to restore the compromised data. Here, data security and data protection work together. Another example could be a data loss prevention policy that prevents users from hosting the personal data of third parties on their laptops or mobile devices—this is an example of a data privacy. Should a user still be able to do this, the laptop can be encrypted or remotely wiped if compromised to prevent the data from being disturbed.

To further elaborate, data security involves three core elements of what is referred to as the CIA triad security model:

- **Confidentiality:** Ensures that data is only accessed by authorized individuals.
- **Integrity:** Ensures that data is trustworthy, accurate, and authentic by retaining it in a pristine and untampered state.
- **Availability:** Ensures that data is available to those that need it to do their job.

For a data-related cyberattack to be successful, it must violate at least one of these CIA elements. Therefore, you need a multi-layered security policy or defense strategy to effectively secure and protect your data from cyber threats.

STATES LEADING THE CHARGE FOR DATA SECURITY COMPLIANCE

There's another reason why organizations are placing a greater emphasis on data security—government regulatory compliance. California was the first U.S. state to follow the example of the European Union's General Data Protection Regulation (GDPR). The California Consumer Privacy Act (CCPA) was passed in 2018 and went into effect January 1, 2020. The law gives California residents greater control over their private information. Like GDPR, the scope of CCPA regulatory coverage applies to any company that manages the data of California resident, regardless of its geographical location. Since CCPA was passed, a host of other states including Nevada, Colorado, New York, and Virginia have followed suit and successfully passed their own regulatory measures—all of which include steep fines.



THE IMPORTANCE OF A STREAMLINED DATA SECURITY STRATEGY

There is no arguing that IT leaders must emphasize data security to protect their increasingly complex IT landscapes, but a greater focus doesn't necessarily mean spending more money, either. The strategy of purchasing additional security tools upon the discovery of a new attack methodology is quickly proving to be non-productive. Many data breaches can be prevented by applying an available patch created for the designated vulnerability. Surveys have shown that as much as 30% of all new security investments are underutilized, or sometimes not even used at all.¹²

According to ESG Research, 31% of organizations use more than 50 different cybersecurity products while 60% use more than 25 products.¹³ More tools will create unnecessary complexity, resulting in the exponential increase of management consoles, logs, and alerts that consume the attention of internal staff. These diminishing returns were made evident in the Cisco 2020 CISO Benchmark Report that exposed the following correlation:¹⁴

- **81%** of organizations that utilized 50+ security vendors had 10,000+ records impacted.
- **54%** of those that utilized 6-10 security vendors had 10,000+ records impacted.
- **35%** of those that utilized 2-5 security vendors had 10,000+ records impacted.
- **16%** of those that utilized 1 security vendor had 10,000+ records impacted.

You don't necessarily need more tools to secure your data, but what you do need is a strategy. This premise is being recognized by state governments as well. One example is Connecticut's Safe Harbor Regulation that was passed in summer 2021. The new law creates a safe harbor (pun intended) for companies that implement reasonable cybersecurity controls, providing them immunity to punitive damages brought against them because of a cybersecurity incident. A company can attain Safe Harbor status by proving that it created, maintained, and complied with a written cybersecurity program that incorporates appropriate technical and administrative safeguards. The program must conform to a cybersecurity framework such as the NIST standards or other industry recognized standard. The courts have also ruled in favor of companies that can prove their "duty of care" in matters of data breach litigation.

A data security strategy should be centered around a zero trust security featuring these five fundamental assertions:¹⁵

1. The network is always assumed to be hostile.
2. Internal and external threats always exist on the network.
3. Network locality is not sufficient for deciding trust in a network.
4. Every device, user, and network flow is authenticated and authorized.
5. Policies must be dynamic and calculated from as many sources of data as possible.



A sound data security strategy should include the following security tools, protocols, and policies:

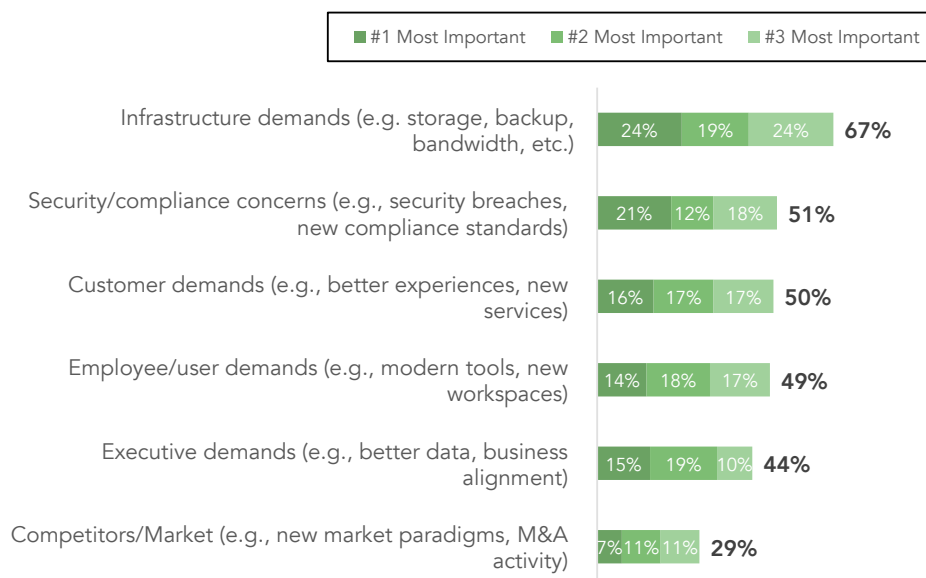
- A next generation firewall at the network perimeter is essential to be able to monitor and filter network traffic.
- The memberships of highly privileged groups should be monitored to be made aware of changes.
- Firewalls should also be incorporated throughout the internal network to enforce network segmentation and to compartmentalize traffic.
- Identity and access management (IAM) measures should be implemented in conjunction with role-based access controls (RBAC) to enforce authentication and authorization. Also ensure that only authorized users can access or transfer data.
- Larger enterprises should utilize AI and ML-driven security systems that can actively identify threats in real time and remediate them in automated fashion.

Additionally, organizations need to have data erasure tools in place that delete data from mobile devices that are potentially compromised. A cyber recovery plan should also be implemented to ensure that data can be restored to its original state if its integrity or condition is corrupted. The cyber recovery plan must include the necessary measures to secure the data backups. This plan should not be confused with a disaster recovery plan.

CYBERSECURITY: A TOP DRIVER OF DIGITAL TRANSFORMATION

As stated earlier, a legitimate data security plan should be part of any enterprise’s digital transformation initiative. In the Foundry (formerly known as IDG Communications) study we mentioned, survey participants were asked to list the top drivers for their digital transformation initiatives. More than one in five individuals had listed security and compliance concerns as their most important initiative with more than half of those individuals also asserting it as one of their top three concerns. See below:

Top Drivers of Digital Transformation





ABOUT WEI

WEI is an innovative, full service, customer centric IT solutions provider.

**Why WEI? Because we care.
Because we go further.**

At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further. And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 30 years.




SECURE YOUR DATA WITH WEI

Speak with our seasoned data security specialists who can analyze both your business objectives and security risks to create a duty of care strategy that not only reduces your enterprise's exposure to the risk of attack, but also the risk of business disruption, noncompliance and litigation. Data security and digital transformation go hand in hand – WEI can show you how.

 info@wei.com

 800.296.7837

 www.wei.com

 43 Northwestern Drive
Salem, NH 03079

Sources:

1. Here's how much ransomware attacks are costing the American economy (cnbc.com)
2. As the cyber insurance bubble begins to burst, the market scrambles for a new approach (scmagazine.com)
3. Lloyd's of London: Cyber Insurance Will Not Cover Cyber Attacks Attributable to Nation-States - CPO Magazine
4. AIG reducing cyber limits as costs climb | Insurance Business America (insurancebusinessmag.com)
5. Sharply Rising Cyber Insurance Claims Signal Further Risk Challenges (fitchratings.com)
6. Global cyber insurance pricing spikes 32% – report | Insurance Business America (insurancebusinessmag.com)
7. <https://www.forbes.com/sites/danielnewman/2017/04/18/agility-is-the-key-to-accelerating-digital-transformation/>
8. Ransomware cyberattacks surged in 2021 according to a new report | Fortune
9. Data breaches break record in 2021 - CNET
10. Ponemon Institute: Cost of Data Breach Hits Record High (secureworld.io)
11. Data Matters Privacy Blog Data Breaches are More Expensive than Last Year, New IBM Security Report Finds - Data Matters Privacy Blog (sidley.com)
12. A Lot of Security Purchases Remain Shelfware (darkreading.com)
13. ESG Research Insights Paper: Toward Enterprise-class Cybersecurity Vendors and Integrated Product Platforms
14. Cisco 2020 CISO Benchmark Report
15. Zero Trust Networks: Building Secure Systems in Untrusted Networks, Even Gilman and Doug Barth