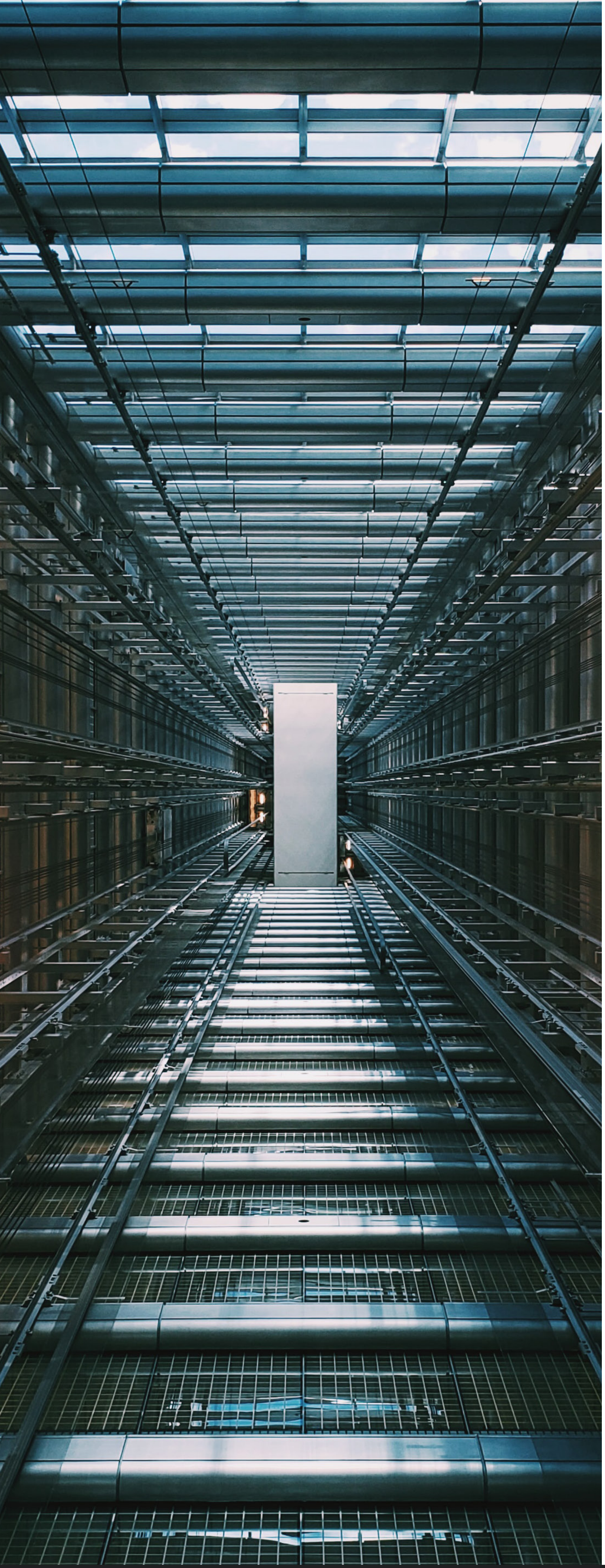
CHECK PLEASE!

How Restaurant, Retail and Hospitality Businesses are Managing Cybersecurity Risks

An independent study commissioned by FreedomPay and Cornell reveals unique insights into the management of cybersecurity by small, medium, and large-size enterprises

FREEDOMPAY

Nolan
Cornell
SC Johnson College of Business
CENTER FOR HOSPITALITY RESEARCH



THE TIME IS NOW

A look into how companies need to optimize cyber-innovation and prioritize cybersecurity systems

The technological revolution and the global pandemic have created a perfect storm for one of the biggest challenges facing merchants today: how to smash channel siloes and join operational dots to deliver seamless integration of physical and digital services in a safe and smart way.

To deliver services safely, merchants rely on cybersecurity systems that can become vulnerable to data breaches if not re-evaluated periodically. Historically, however, the complexity, impact to operations, and cost of re-evaluating security systems has made merchants across most industries, particularly retail, apprehensive to do so. This report reveals that thinking has changed post COVID-19 whilst the response remains confused. Merchants experienced a surprising number of hacks and multiple breaches to systems and data despite increased investment and strong awareness. What could be the reason? Perhaps, an increasing number of merchants are struggling with the safeguard and execution of intelligent customer data and customer visibility. Or the task of implementing more advanced technology to gain that visibility is too great.

Whatever the reason, the irony is that if businesses don't act now and re-evaluate their entire end-to-end systems, standing still will only increase their vulnerability to data attacks and other security concerns, while at the same time risk losing customer loyalty and trust.

This report is just a snapshot of views toward cybersecurity in America's business eco-system. That said, we believe it illustrates the challenges, opinions and actions merchants of all sizes are facing. Read the report to find out how cybersecurity is being tackled and prioritized as the world shrinks, and hackers and consumers become savvier.

> *"Indeed, this report reveals several interesting results including a* ***surprising number of hacks and multiple breaches to systems and data*** *despite increased investment and strong awareness post COVID-19."*

CHRIS KRONENTHAL

FREEDOMPAY
PRESIDENT

CYBER CONCERNS IN THIS ERA OF DIGITAL COMMERCE

Recent advancements in technology have allowed the hospitality, retail, and food and beverage industries to better serve the needs of their customers in a digitized era. Companies have optimized their systems to meet the growing demand for user-friendly virtual access to various goods and services, with several moving entirely online in recent years. Many larger businesses are leveraging data collection and analytics tactics to create more personalized user experiences and marketing for customers.

IBM Security: The Cost of a Data Breach Report 2021

$4.24m
in data breach costs

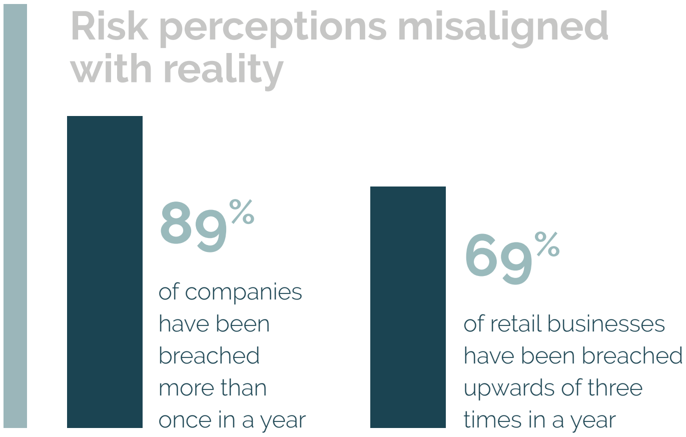
$10%
increase in average total cost of a breach from 2020 - 2021

$1.7m
cost difference where remote work was a factor in breach

The COVID-19 pandemic marked a turning point in this era of digital commerce, accelerating an already increasing trend in global retail trade. Amidst stagnant economic activity, global lockdowns induced by COVID-19 brought leading companies in the United States to implement eCommerce, teleworking, and cloud computing solutions. According to the United Nations Conference on Trade and Development, online activity by businesses and consumers raised eCommerce's share of global retail trade from 16% to over 20% in 2020. While overall retail sales declined by 1% in leading business-to-consumer countries, online retail grew by 22%. In line with this salient trend, eCommerce sales within the United States soared from $598 billion in 2019 to $792 billion in 2020.

While this shift towards online retail has accelerated the digital growth and accessibility of the online service industry, it also raises a slew of cyber concerns for companies.

As services become increasingly digitized, companies must contend with customer and stakeholder demands to protect their systems and data from cybersecurity attacks like phishing, hacking, and malware. Service providers have always had to withstand the threat of security breaches. Yet as the ongoing COVID-19 pandemic pushed more businesses to turn to eCommerce, these threats have become more and more common. Experts acknowledge that companies and users are now more susceptible to cyber exploitation than ever before, with economic instability increasing online criminal activity and heightening the vulnerabilities of employees working from home.



According to a report from IBM Security with the analysis of data compiled by the Ponemon Institute, **the average total cost of a data breach increased by nearly 10%** year over year, the largest single year cost increase in the last seven years, with a **$1.07m** cost difference where remote work was a factor in causing the breach.*

*IBM Security. 2021. Cost of a Day Break Report 2021. IBM Corporation. https://www.ibm.com/security/data-breach

As many cyber-attacks result from user activity rather than breaches in company systems, retail customers are particularly at risk of exposure to cyber threats. Cyber-attackers specifically have leveraged the pandemic as an opportunity to take advantage of users' interest in COVID-related information, spreading malware and ransomware, launching phishing schemes, and swiping login credentials through malicious fake websites and pandemic news simulations. With the hospitality industry, in particular, platforms that rely on customer data to maintain an edge over competitors are particularly vulnerable to sophisticated forms of machine learning-based cyber exploitation that target guest and user information. Due to the sensitive nature of user data in the hospitality industry, experts urge professionals to enlist a range of user-friendly preemptive measures that strengthen security barriers and protect customer interactions.

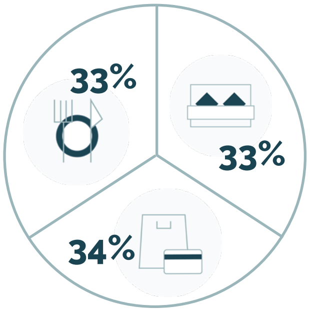
Cyber-attackers specifically have ***leveraged the pandemic as an opportunity*** *to take advantage of users' interest in COVID-related information,* ***spreading malware and ransomware, launching phishing schemes, and swiping login credentials*** *through malicious fake websites and pandemic news simulations.*

Nevertheless, stakeholder attitudes surrounding cyber-innovation and company usage of cybersecurity vary across industries and enterprises, and many companies have yet to optimize their cybersecurity systems. As such, FreedomPay and Cornell's Center for Hospitality Research commissioned the **Cybersecurity Attitudes & Usage Survey** to understand these trends and variations, focusing on current cybersecurity behaviors, barriers to optimization, customer experiences, and the future of cybersecurity practices.

Hanover Research recruited a total of 300 respondents through a panel and administered the survey online. Respondents were all adults living in the United States who had full-time employment working in the Hospitality, Retail, or Food and Beverage Industry in companies with at least 50 employees and minimum annual revenue of $1 million. All respondents had primary or shared decision-making authority for purchasing cybersecurity products at their company and were thus best-suited to address the research questions:

Key Segmentations

This analysis includes questions segmented by industry and merchant size.

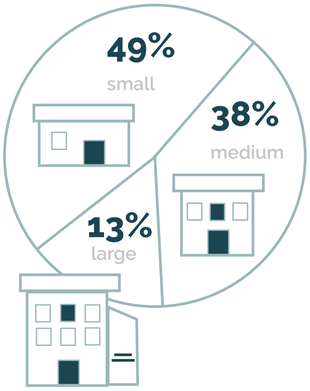


Industry (n=300)

Food & Beverage (n=99)

Hospitality (n=100)

Retail (n=101)



Merchant Size [Revenue] (n=300)

Small [$1 mil - $249 mil] (n=147)

Medium [$250 mil - $999 mil] (n=115)

Large [1 bil or more] (n=38)

- What cybersecurity systems are merchants currently using?
- How optimized are their cybersecurity systems?
- What are the factors that are inhibiting them from moving from their current system to the optimal system?
- What are the expectations of and reassurances for customers?
- What are the underlying issues impacting cybersecurity issues?

What follows are highlights from Hanover's findings organized by specific cybersecurity challenges, systems in place that address these challenges, and stakeholder responses to cybersecurity measures. Finally, recommendations are found in the conclusion, which reflects how companies and consumers prioritize safety and security in their services.

*Stakeholder attitudes surrounding cyber-innovation and company usage of cybersecurity vary across industries and enterprises, and **many companies have yet to optimize their cybersecurity systems**.*

KEY FINDINGS

Small businesses are more likely to keep security systems housed under a single department than large enterprises with multiple departments involved. **82%** of retail companies use network security.

Cybersecurity Threats

External threats make up **82%** of the factors likely to negatively impact a company's security system. Over half of companies cite payment integrity and malware as major cybersecurity concerns, and risk management remains their systems' most significant challenge. Food and beverage companies, in particular, are challenged with data mismanagement in comparison to larger retail enterprises that more often contend with hackers, data loss, and phishing attacks.

Nearly **one-third (31%) of companies** have experienced some **data breach** in the past.

Cloud Security

Most companies utilize a cybersecurity system for cloud security and network, customer data, and payment security. Three-quarters of companies employ more than one cybersecurity system, with medium-sized businesses **(80%)** being substantially more likely to do so than small businesses **(67%)**.

Reliance on Third-party Suppliers

Many companies rely on third parties to manage and secure user information because they are better equipped to meet company needs. **Two-thirds** of companies either solely contract third-party supplies or secure information both in-house and externally. While companies that utilize third-party service providers often vet them to ensure that their employees receive adequate training, they ultimately trust these external suppliers because they provide superior and cost-effective services.

Food and beverage and hospitality companies primarily rely exclusively on third-party suppliers, significantly more than retail companies; **half** of retail enterprises use a combination of in-house and third-party contracts. **41%** of small businesses use third-party suppliers compared to **30%** of medium and **21%** of large enterprises.

Cybersecurity Budgets

Retail companies devote over **41%** of their budget to cybersecurity, compared to food and beverage and hospitality companies, which portion **12%** of their annual budget to these efforts. Half of the companies have increased their IT budget since 2019, though these increases have been relatively small.

Respondents estimate that their companies spend close to one-quarter of their budget on security systems, an appropriate amount to optimize cybersecurity.

Show Me the Money

83% of companies who use third-party suppliers to manage and secure information say its **"more cost-effective"** for their business

51% of companies who do not use a third-party supplier cite it as being **"more costly"** than their current process

Budgetary concerns may also play a factor in determining any potential system enhancements — **among the few (15%) that currently do not have plans to enhance their system**, they are most likely to **cite preventative costs (61%)** and an **unwillingness to have a disruption in service (52%)**

Conferences and Seminars

71% of companies rely on conferences and seminars to train and engage end-users in cybersecurity. This form of user-end engagement is most common at small- and medium-sized companies, where merchants are significantly more confident than their counterparts at large enterprises that rely on training videos.

Stakeholder Satisfaction

Around **95%** of internal stakeholders are satisfied with their company's systems and internal risk assessment processes, but they still want to improve their systems.

Merchants have faith in their cybersecurity systems because they employ the latest security features and technological processes and invest in their optimization. The majority of merchants are confident that their company's systems are optimized to meet all security challenges.

Still, **85%** of companies plan to enhance their system, and two-thirds have upgraded their system within the past year, resulting in over half expanding their customer base size.

Retail companies are more likely than hospitality and F&B companies to enhance their security procedures, while **64%** have upgraded within the past year. **21%** of small businesses have no plans to improve their system, which is significantly higher than medium or large businesses. The few that currently do not intend to enhance their system are likely to cite financial costs and disruption in service as preventative factors.

Prioritizing Cybersecurity

Companies prioritize cybersecurity and want their customers to feel secure in using services. **96%** of companies value cybersecurity systems' role in protecting company and user data. The vast majority of companies believe that their customers would be more loyal, reassured, and satisfied with additional security measures. Over **70%** of companies believe that customers want their data and payment to be secured. Still, **two-thirds** believe that customers seek user-friendly systems and are annoyed by extra security (e.g., two-factor authentication). more than retail companies; **half** of retail enterprises use a combination of in-house and third-party contracts. **41%** of small businesses use third-party suppliers compared to **30%** of medium and **21%** of large enterprises.

A Balancing Act

91% of companies believe their customers deeply care about cybersecurity

86% of companies believe it increases customer loyalty

65% of leaders believe that customers are annoyed by extra security measures

67% of leaders believe that customers want systems to be easy to use

U.S. Government Role

The majority of companies appear to welcome support from the U.S. government in fighting cyber threats and enhancing cybersecurity policies. Large enterprises and retail companies are less likely to want such intervention, but a majority (around three-quarters) is open to involvement.

Recommendations

Given these findings and understanding of market attitudes for small, medium, and large-sized businesses across three industries, we offer several key recommendations for service providers and professionals:

- Customers value cybersecurity and safe transactions, so extra security measures will enhance the user experience and promote respect, loyalty, and satisfaction. Therefore, companies should **advance cybersecurity systems in a place visible to customers.**

- Two-thirds of companies already work with a third-party supplier for efficient and cost-effective data management and security services. Companies should aim to **emphasize the value of working with a third party.**

- Implementing the latest security features and processes is the best way to combat the possibility of external threats. Merchants should **ensure that software, hardware, and firmware are always up-to-date.**

- The majority of companies are open to further support from the U.S. government. Companies and leaders should **encourage government involvement in fighting cyber threats and enhancing cyber-security policies.**

These recommendations underscore the relevance of cybersecurity systems in meeting the adapting needs of consumers and companies in a data-driven digital era. Small, medium, and large businesses in the F&B, hospitality, and retail sectors have varying approaches toward cybersecurity tactics. Still, all emphasize the importance of such measures in protecting vital information and enhancing customer satisfaction.

ADDITIONAL INSIGHTS

In the Dark

More than **one-third (35%)** of surveyed leaders **do not know how much** of their company's budget is spent on cybersecurity.

Dual Opinion

While **91% of respondents agree** that their customers **do care** about cybersecurity, **48%** also believe their customers **do not care** about cybersecurity.

Inaction

Nearly all (96%) companies say they **value the importance of security systems to protect their data**, and **85% agree that their customers would be more satisfied if they had extra security measures in place.** Yet, **half (50%)** have either not increased their IT security budget or decreased their budget since 2019.

Checking the box?

91% of merchants are **very** or **extremely confident** that their company adequately trains end-users

71% of merchants rely on conferences and seminars to keep them trained and engaged

Notably, **small (92%) and medium (95%)** merchants are significantly more confident than their **large (79%)** counterparts, where the most common form of end-user engagement comes from training videos **(82%)**

Looking for a Leader

87% of companies say they would welcome involvement from the U.S. government to fight cybersecurity threats

84% of companies say they would welcome involvement from the U.S. government to enhance policy

Large merchants **(threats - 76%, policy - 74%)** and retail companies **(threats - 81%, policy - 75%)** are significantly less likely to want the U.S. government involved

FreedomPay is the world's leading consumer-centric commerce payments platform specializing in the hospitality industry. FreedomPay has collaborated with the The Cornell Peter and Stephanie Nolan School of Hotel Administration, the world's leading hub for research in the business of hospitality.

FREEDOMPAY | Nolan
Cornell
SC Johnson College of Business
CENTER FOR HOSPITALITY RESEARCH

About The Author

Prameela Kottapalli is a staff writer for the Cornell SC Johnson College of Business Centers & Institutes. She is a sophomore majoring in the College Scholar Program in Cornell's College of Arts & Sciences. She is part of several initiatives including migrant justice advocacy, leadership of her professional fraternity and social sorority, Outdoor Odyssey, and the Meinig Family Cornell National Scholars Program. She is passionate about telling unique stories and enjoys writing about the cutting-edge innovation of the Centers & Institutes.