DARK Reading

REPORTS

October 2021

How Data Breaches Affect the Enterprise

Data breaches continue to cause negative outcomes for organizations. Could a decline of major impacts indicate companies are getting better at containing data breach fallout?

Sponsored by VULCAN.

informa tech

TABLE OF CONTENTS

Figures

Remediation
Summit 2021

Previous Next

Table of Contents

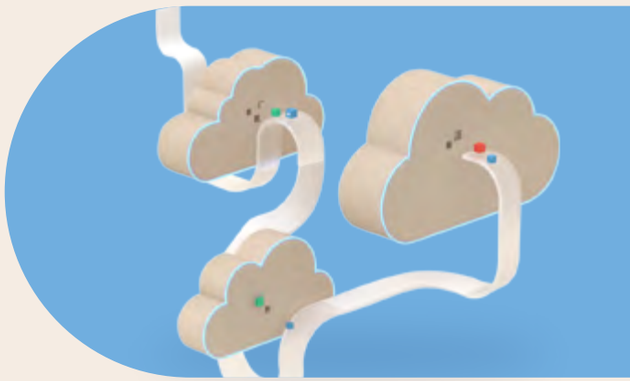
Attend The Remediation Summit 2021

Dec 9, 2021
100% Virtual | 100% Free

Bringing you the leading minds, best practices and latest technologies in cyber risk measurement, vulnerability prioritization and remediation.

REGISTER NOW



FEATURING EXPERT SPEAKERS FROM: zoom BEST BUY DataRobot

VULCAN.

About the Author

Jai Vijayan
Dark Reading

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He specializes in writing on information security and data privacy topics. He was most recently a Senior Editor at Computerworld. He is a regular contributor to Dark Reading, CSO Online, and TechBeacon.

EXECUTIVE SUMMARY

Data breaches caused network disruptions and application outages at many organizations over the past year. A substantial number of organizations report experiencing financial losses of varying severity, fraud, negative publicity, brand erosion, and several other consequences after a data breach. However, with a few exceptions, the proportion of organizations reporting major impacts declined significantly compared with a year ago, suggesting that many have gotten better at containing breach fallout.

Dark Reading surveyed 150 technology and cybersecurity professionals on a range of topics pertaining to the threat landscape and how it has affected them. The objective was to understand the impact of data breaches on enterprises and what security and IT teams are doing to protect against similar incidents in the future. Respondents included IT and security decision-makers and practitioners at organizations with 100 or more employees from across more than 18 industries.

The responses show a majority expect to experience a major data breach over the next 12 months. The rapid growth of ransomware and the increased volume of cyberattacks overall have left many organizations feeling more vulnerable to a data breach than a year ago. Security compromises over the past year at organizations such as SolarWinds and Colonial Pipeline have heightened concerns about hackers sponsored by nation-states, especially groups based in Russia. A significantly higher proportion of IT and security leaders compared with a year ago are concerned about breaches involving the misuse of credentials belonging to privileged users and administrators.

Phishing, malware, and denial-of-service attacks were the most common causes for data breaches. Fewer organizations this year report targeted attacks as a cause for a data breach compared with either of the previous two years. One possible reason may be because threat actors resorted to more opportunistic attacks in the wake of the pandemic-induced shift to a more distributed work environment. Despite heightened concerns over ransomware, fewer organizations in our survey this year report being an actual victim of a ransomware attack. But one-third of those who did get hit by ransomware paid a ransom to restore access to their data.

As we saw in previous Dark Reading Strategic Security Surveys, security and IT decision-makers perceive cybercriminals and users with authorized access to the network as the biggest breach threat. The high volume of publicly disclosed data breaches over the past year have pushed organizations to deploy a multi-tiered approach to protecting data and applications from attack and compromise. Most survey respondents express confidence in their preparedness to respond to a data breach or ransomware attack.

Here are some key data points from the survey:

- 23% of organizations that experienced a data breach over the past 12 months report network disruptions and application unavailability; 17% say they experienced a major financial loss, and 15% report fraud.
- 16% of survey respondents describe their organization as being more vulnerable to a data breach compared with a year ago; 56% say their exposure has remained unchanged.
- 48% of respondents say that if their organization experiences a major data breach in the next 12 months, the most likely cause will be a negligent end user.
- 67% of IT and security decision-makers point to increased attack volumes as the primary reason for their increased vulnerability to a data breach.
- 33% of organizations that experienced a ransomware attack ended up paying a ransom to get their data back, but only 4% report being victimized by a ransomware attack, compared with 13% last year.
- 70% IT and security decision-makers describe the attacks on Colonial Pipeline and JBS as heightening ransomware fears.
- 60% of respondents are confident about their organization's ability to respond to a data breach; 59% believe their organization has an effective strategy for responding to a ransomware attack.

SYNOPSIS

RESEARCH

Survey Name: Dark Reading 2021 Strategic Security Survey

Survey Date: August 2021

Number of Respondents: 150 technology and cybersecurity professionals at companies of all sizes from a variety of industries. The margin of error for the total respondent base (N=150) is +/-7.9 percentage points.

Methodology: The survey queried decision-makers with job titles that involve IT or IT security (cybersecurity) at organizations across more than 18 industry sectors. One-third (33%) have director or head job titles on the IT or security side; 14% have CIO, CTO, CSO, or CPO titles. The survey was conducted online. Respondents were recruited via email invitations containing an embedded link to the survey. The email invitations were sent to a select group of Informa Tech's qualified database; Informa is the parent company of Dark Reading. Informa Tech was responsible for all survey design, administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.

ABOUT US

Dark Reading Reports offer original data and insights on the latest trends and practices in IT security. Compiled and written by experts, Dark Reading Reports illustrate the plans and directions of the cybersecurity community and provide advice on the steps enterprises can take to protect their most critical data.

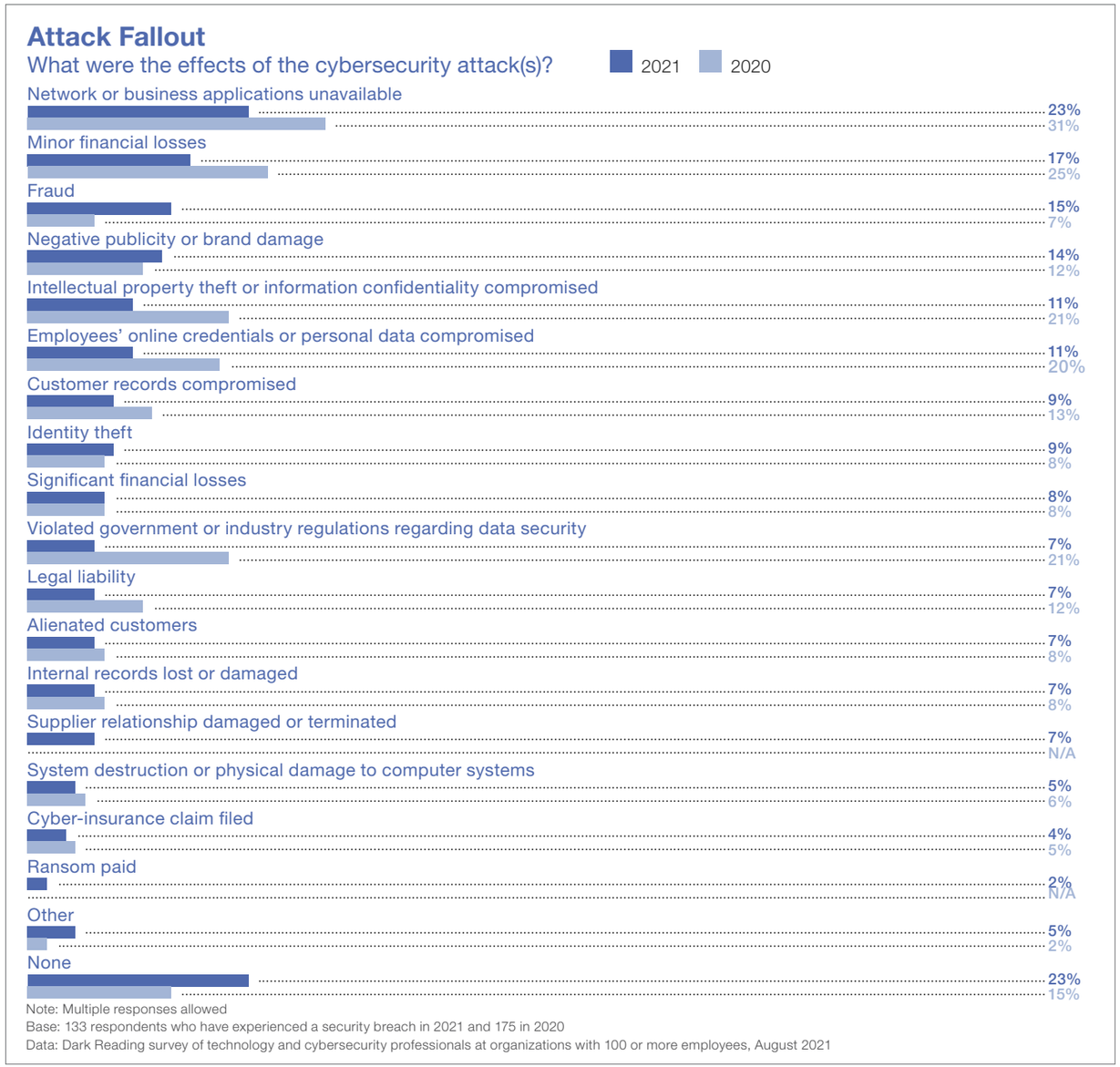
Dark Reading Reports

The Varied Effects of Data Breaches

Just as data breaches can have multiple causes, the impacts from one can be varied as well. The fallout from a data breach can range from the relatively minor and inconsequential to major business disruptions with steep financial consequences for victim organizations.

Dark Reading's 2021 Strategic Security Survey shows that nearly a quarter (23%) of organizations that experienced a data breach over the past year contended with disruptions to their network and to application availability **(Figure 1)**. Seventeen percent report the disruptions as resulting in minor financial losses, and another 8% say they had experienced significant financial consequences because of a data breach. Instances of organizations experiencing fraud after a data breach more than doubled from 7% in our survey last year to 15% this year. The percentage of organizations reporting negative publicity or brand damage after a data breach ticked upward as well, from 12% last year to 14% this year.

Figure 1.



Note: Multiple responses allowed
Base: 133 respondents who have experienced a security breach in 2021 and 175 in 2020
Data: Dark Reading survey of technology and cybersecurity professionals at organizations with 100 or more employees, August 2021

Generally, though — except for fraud and negative publicity — fewer organizations compared with last year's survey report experiencing significant fallout from a data breach. For example, 31% and 25% of respondents last year reported network problems and financial loss following a data breach, compared with 23% and 17%, respectively, this year. Similarly, fewer organizations (11%) report intellectual property theft or compromise of information confidentiality, compared with last year's 21%. There were similar declines in the percentage of organizations reporting other data breach impacts. For instance, fewer respondents (11%) report credential theft this year compared with our previous survey (20%). The percentage of organizations that fell afoul of regulatory requirements because of a data breach dropped from 21% last year and 12% in 2019 to just 7% this year, while those reporting compromised customer records went from 13% in 2020 to 9% in our latest survey.

The data — on the surface, at least — would suggest that many organizations are getting better at containing breach fallout. Indeed, 60% describe their organization as being well-prepared when asked to evaluate their capabilities for responding to a breach in the coming year **(Figure 2)**. An almost identical number (59%) say their organization has an effective strategy for responding to a ransomware attack.

At the same time, other studies have shown that consequences are getting worse for organizations that have not implemented adequate measures for mitigating the effects of a breach. The 2021 edition of IBM's widely quoted "Cost of Data Breach Report" showed the average cost of a data breach for organizations increased 10% over last year, from $3.86 million to $4.24 million. The increase was the biggest over a 12-month period in seven years and highlights the big impact that a major breach can have on organizations that have not implemented a mature process for responding to a security incident. IBM's study found that the average cost of a data breach was more than $1 million higher for companies that had a remote workforce. Some 17.5% of the breaches analyzed in the study involved companies with remote workers,

As has been the case for some time, more companies (53%) experienced a data breach over the past year because of phishing than because of any other cause **(Figure 3)**. The percentage of organizations reporting a phishing-related compromise was marginally higher than last year's 51% and shows once again just how challenging the phishing problem remains for many organizations. In fact, 36% of the breaches that Verizon's breach investigations team responded to in 2020 involved phishing — up 11 percentage points from 25% of breaches in 2019. Verizon attributed the sharp increase to attackers trying to take advantage of increased vulnerabilities stemming from the shift to large-scale remote work because of the COVID-19 pandemic. Dark Reading's survey finds that 40% of respondents blame the pandemic for an increase in phishing and social engineering attacks built around the crisis **(Figure 4)**.

Figure 2.

Organizations' Cybersecurity Strategies and Processes

Please rate your agreement with the following statements.

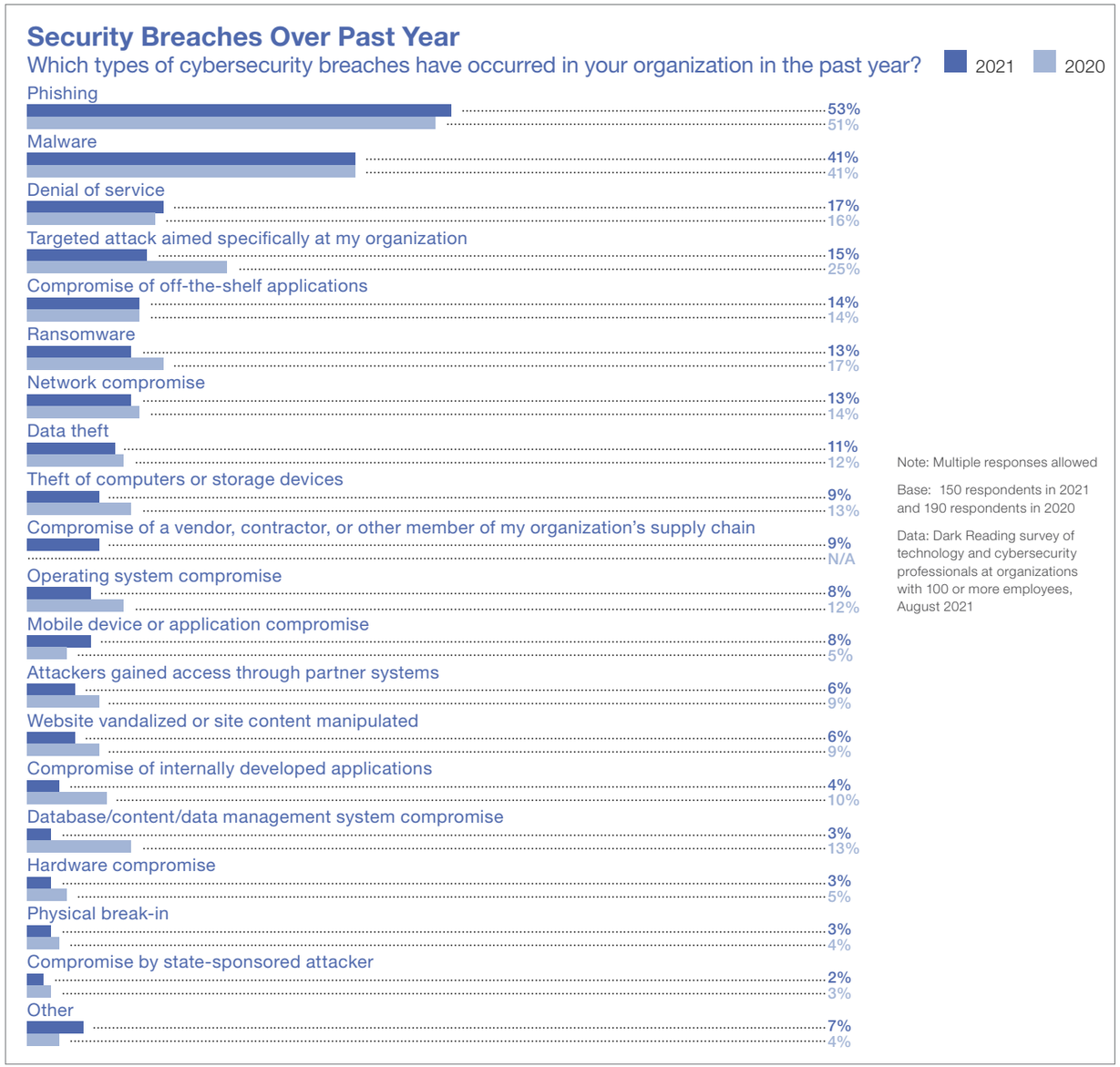
	Strongly agree	Agree	Disagree	Strongly disagree	Don't know
My organization has an effective method for measuring the current state of its security posture	13%	63%	18%	2%	4%
I believe the effects of the COVID-19 pandemic will fundamentally change my organization's computing and data security strategies for the long term	18%	57%	17%	4%	4%
The attacks on Colonial Pipeline and JBS have significantly increased my organization's concerns about ransomware	15%	55%	17%	8%	5%
I believe that my organization's cybersecurity staff are stretched too thin, which may result in burnout and/or increased risk to critical data	28%	42%	22%	5%	3%
My organization has an effective method for measuring the effectiveness/performance of its security department	17%	47%	29%	4%	3%
I believe my organization has an effective long-term strategy for protecting data security handled by home users	19%	44%	25%	6%	6%
I believe my organization will have to respond to a major data breach or compromise in the coming year	18%	44%	16%	5%	17%
I believe my organization is well-prepared to respond to a major data breach in the coming year	16%	44%	27%	5%	8%
I am confident that my organization has an effective strategy for response to a ransomware attack.	14%	45%	26%	5%	10%
I believe my organization has an effective process for measuring the cybersecurity risk that my organization will face in the coming year	11%	48%	29%	5%	7%
Supply chain attacks such as SolarWinds and Kaseya have significantly decreased my confidence in my organization's supply chain security	13%	37%	34%	10%	6%
Since the SolarWinds attack, my organization has initiated significant changes in its approach to supply chain security	3%	43%	32%	9%	13%

Data: Dark Reading survey of 150 technology and cybersecurity professionals at organizations with 100 or more employees, August 2021

Once again, malware was the second biggest cause for a data breach over the past year. Forty-one percent of the organizations in Dark Reading's survey say they experienced a data breach in which malware was the primary infection vector. An identical percentage of survey respondents identified malware as a breach cause last year as well. However, the nature of malware attacks has shifted in focus over the past year. More than 91% of all malware samples are delivered via encrypted traffic these days — a higher percentage than ever before, according to a recent analysis of threat data by WatchGuard. The use of fileless malware by threat actors has soared to all-time highs, and a greater percentage of malware is being directed at remote user endpoints than endpoints behind the enterprise network. The trends have required organizations to refocus and review their malware defenses.

Other relatively common data breach causes over the past year include denial-of-service attacks (17%), compromise of off-the-shelf software (14%), network compromise (13%), and theft of a computer or storage device (9%).

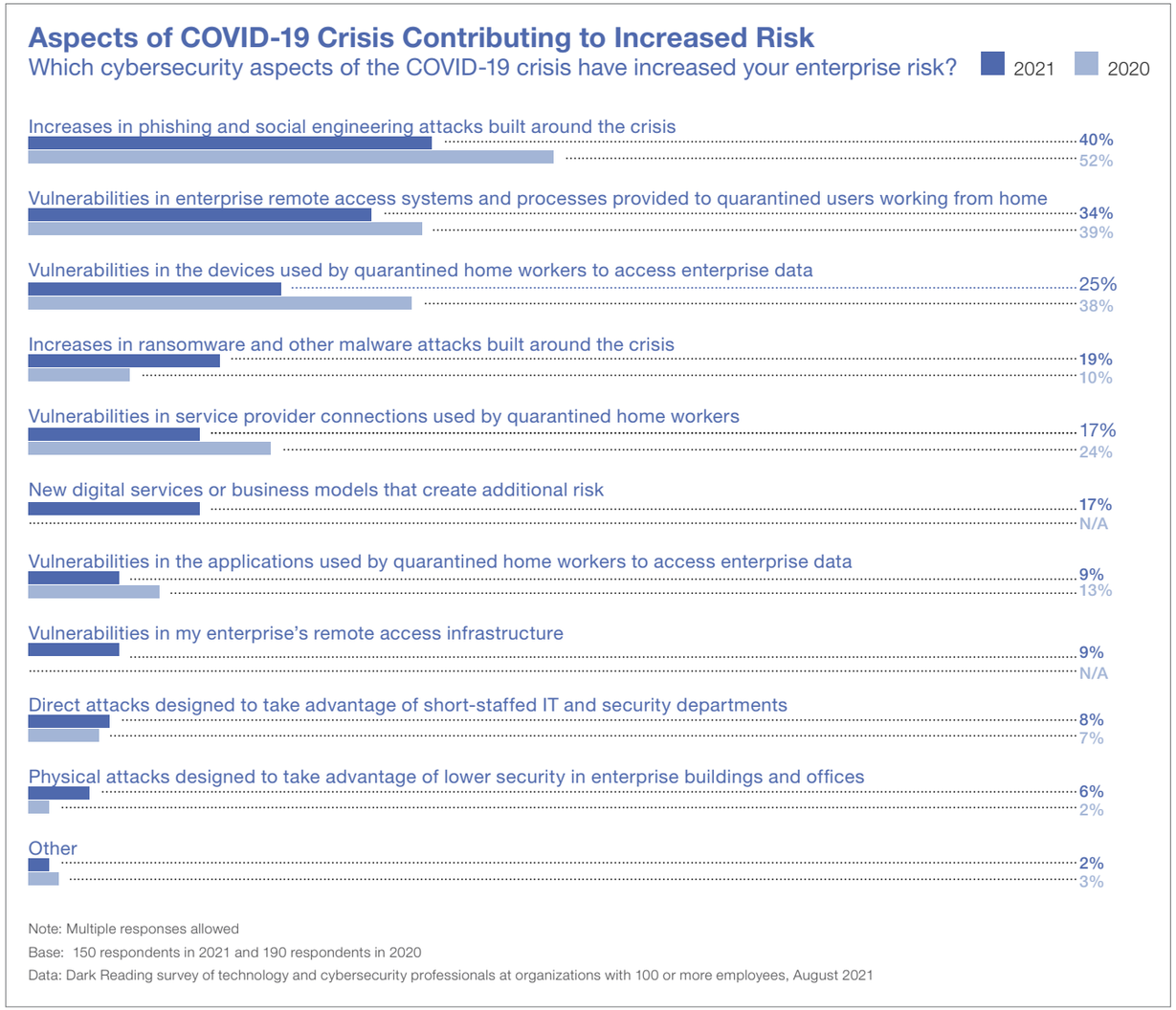
Figure 3.



Significantly, despite heightened concerns over ransomware and targeted attacks, the number of organizations that report a breach stemming from either cause is relatively low. For instance, only 15% of respondents identify their organizations as victims of a targeted attack in the preceding 12 months — the lowest number in the last three years. Last year, 25% of organizations in Dark Reading's Strategic Security Survey reported a targeted attack, and in 2019, the number was 19%. One reason is that attackers — including nation-state actors and organized criminal groups — have switched to more opportunistic targeting of new vulnerabilities caused by the shift to remote work and rapid cloud adoption in the wake of the COVID-19 pandemic. A study that NTT conducted this year found a big 300% increase in such attacks.

Similarly, fewer organizations in our survey this year (13%) say they experienced a ransomware-related breach than in our 2020 survey (17%) and in our 2019 survey (14%). The numbers suggest that concerns over ransomware attacks are higher than actual incidents.

Figure 4.

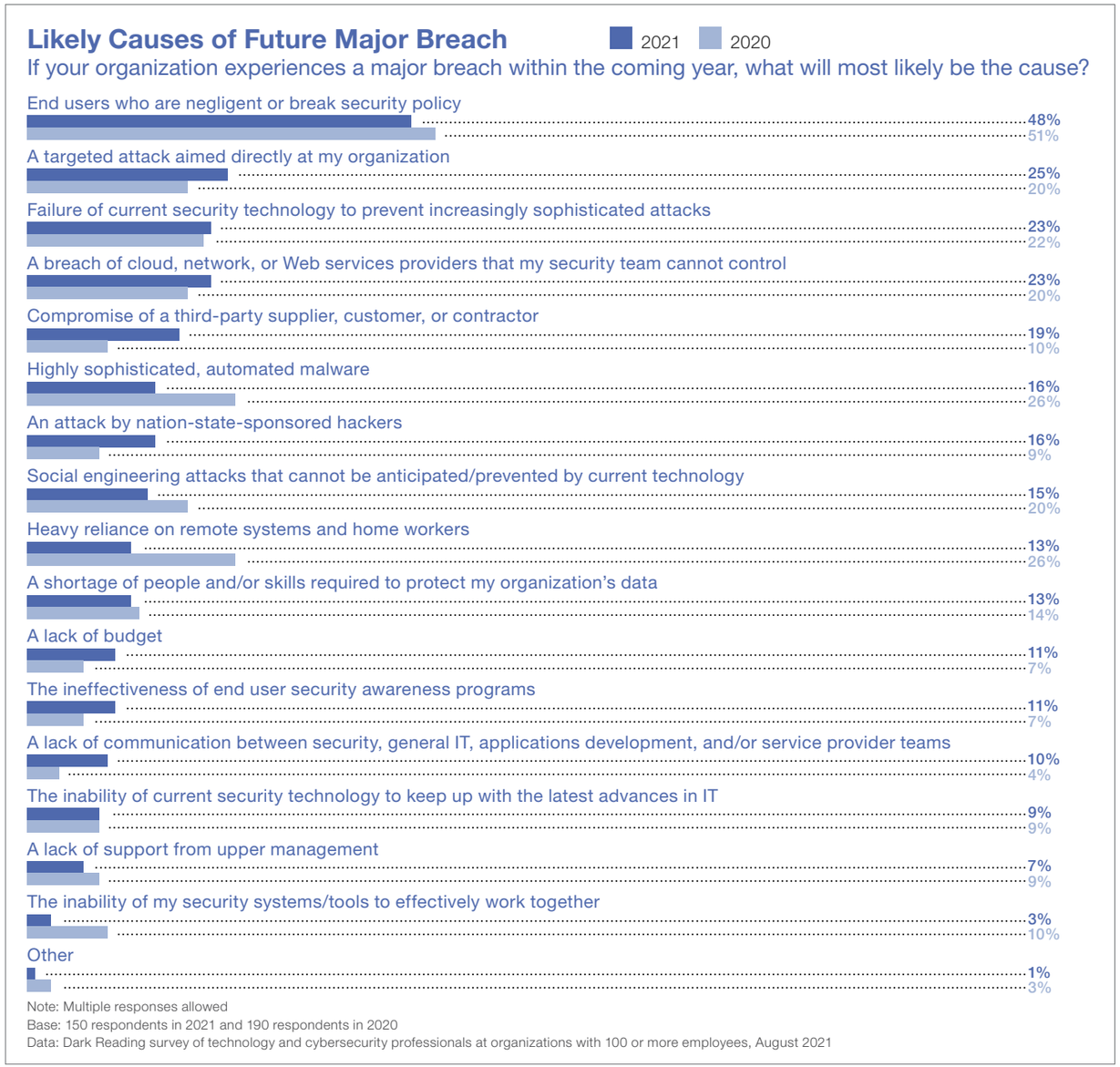


How Breaches Affected Threat Perceptions

The nature of major data breaches over the past year appears to have driven some change in what security and IT managers perceive as big threats to enterprise data and applications. For instance, concerns over attacks by state-sponsored threat actors are significantly higher than in our survey last year and the year before. Sixteen percent of survey respondents expect that if they experience a data breach over the next year, a state-sponsored threat actor would be the cause **(Figure 5)**. That's almost double the 9% of respondents who said the same thing in our past two surveys, even though the number of actual compromises by state-sponsored actors has remained largely unchanged, at around 2% of survey respondents. Concerns over targeted attacks have similarly grown, with 25% citing it as being the most likely cause of a breach over the next 12 months, compared with 20% last year.

The concerns appear to be linked to incidents such as the supply chain compromise at SolarWinds and the ransomware attacks

Figure 5.



on Colonial Pipeline, meat processing giant JBS Foods, and software vendor Kaseya over the past year. The SolarWinds breach resulted in malware being distributed via poisoned software updates to thousands of the company's customers, though only fewer than 100 of them were the actual targets of the campaign. The ransomware attack on Colonial Pipeline triggered a temporary fuel shortage in some parts of the US East Coast, while that on JBS raised the specter of major disruptions to US meat supplies. The assault on Kaseya resulted in ransomware being distributed to dozens of the company's managed service provider customers and, in turn, to thousands of their customers. The US government blamed Russia's foreign intelligence service for the attacks on SolarWinds and Colonial Pipeline. Security researchers have pointed to a Russia link in the Kaseya and JBS attacks as well.

The incidents seem to have had a big effect on the collective psyche of security and IT managers. Fifty-nine percent of the respondents in Dark Reading's survey describe Russian cyberattackers as posing

a serious threat to their specific organization **(Figure 6)**. Seventy percent of organizations are now more concerned about ransomware attacks because of the incidents at Colonial Pipeline and JBS. This despite only 4% report falling victim to a ransomware attack in which data was encrypted and a ransom was demanded **(Figure 7)**.

Meanwhile, the attacks on SolarWinds and Kaseya have significantly eroded confidence in supply chain security at 50% of organizations. Nineteen percent — nearly double last year's 10% — say that if they experience a major breach in the next 12 months, it will likely result from a compromise at a third-party supplier, customer, or contractor. As one survey taker notes: "I think supply chain security is a myth … as we saw with SolarWinds." Organizations can adhere to best practices such as those prescribed in the Cybersecurity Maturity Model Certification (CMMC) standard and ISO 27011. But that still doesn't guarantee security, the respondent says. "That doesn't mean that they might not have an unpatched system in a developer's home that accesses a developer laptop. A scary thought, but right now we live in the Wild West where the borders are blurred and our enterprise network extends to people's homes."

A steady stream of breaches that resulted from other vulnerabilities — such as the so-

Figure 6.

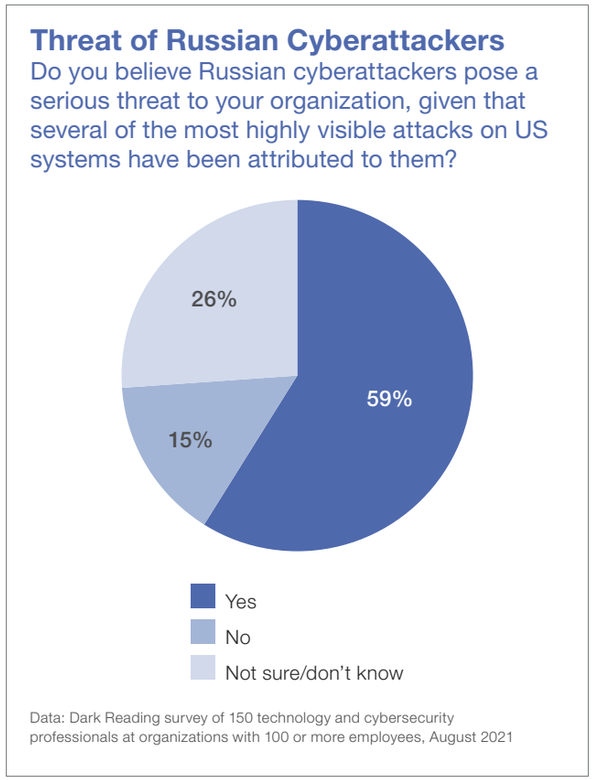
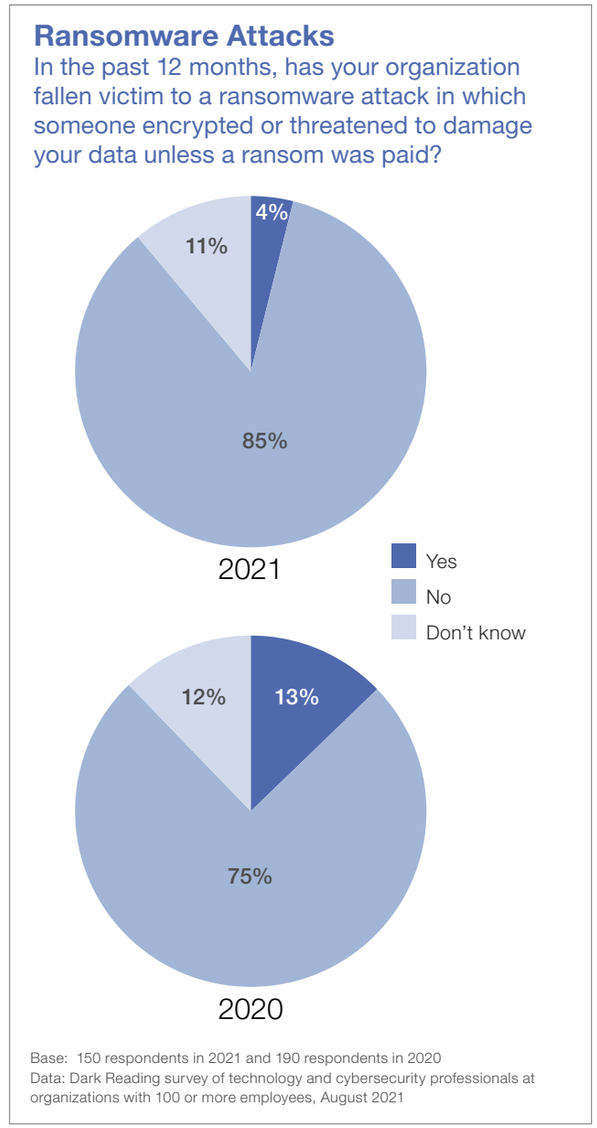


Figure 7.

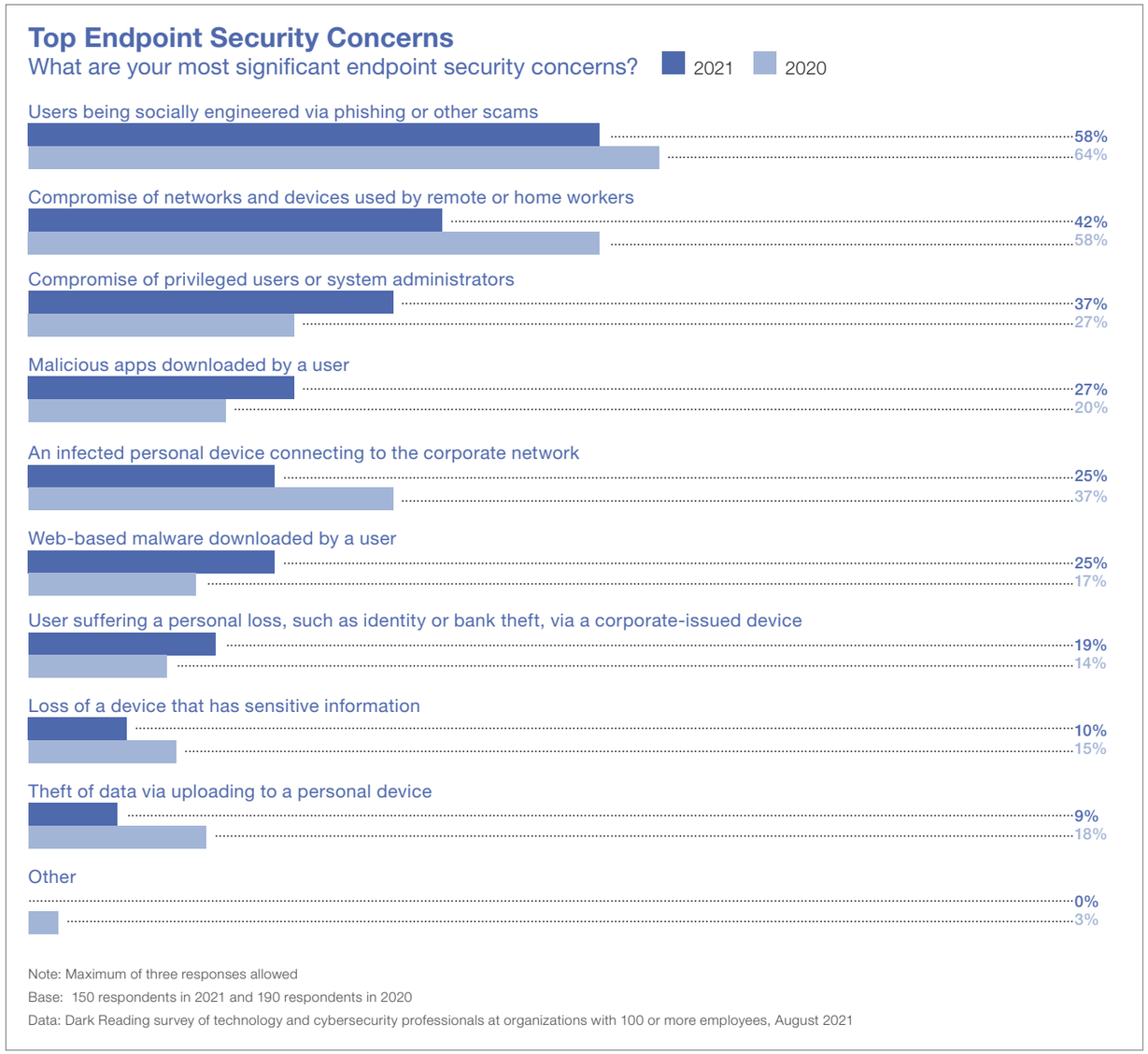


called ProxyLogon set of flaws in Microsoft Exchange Server disclosed in March and multiple previously patched vulnerabilities in VPNs from Pulse Secure and other vendors — appear to have had an effect as well. Thirty-seven percent of survey respondents, compared with 27% last year, now view the compromise of privileged user and administrator credentials as their most significant security concern **(Figure 8)**. Marginally more respondents than last year — 23% compared with 20% — are worried about a breach resulting from the failure of a security technology.

Vulnerabilities and Threats

Security and IT leaders generally appear confident in the multilayered controls they have deployed to prevent, detect, and respond to a data breach. As previously noted, most believe they can respond to a data breach and ransomware attack in an effective manner. Many are using cyber insurance to transfer at least some breach liability to a third party. Fifty-eight percent are covered for cybersecurity breaches either as part of a broader business

Figure 8.



insurance policy or under a specific breach policy **(Figure 9)**. Thirteen percent of those who filed a claim under a breach policy were paid without dispute, and 8% received it after a dispute **(Figure 10)**.

Perhaps as a result of these measures, the percentage of respondents that describe their organization as being more vulnerable to a data breach declined from 23% to 16% compared with a year ago **(Figure 11)**. Those who identify their organization as being more vulnerable point to several factors for their increased discomfort. The chief among them were increased attack volume (67%), increased threat sophistication (56%), growth in ransomware attacks (56%), and a shortage of skilled security staffers (56%) **(Figure 12)**. Our previous surveys have identified all of these issues as primary contributors to feelings of increased breach vulnerability among security executives and practitioners.

Concerns over new vulnerabilities tied to the COVID-19 pandemic response remain high, but not to the same extent as last year. For example, in our 2020 survey, 56% of

Figure 9.

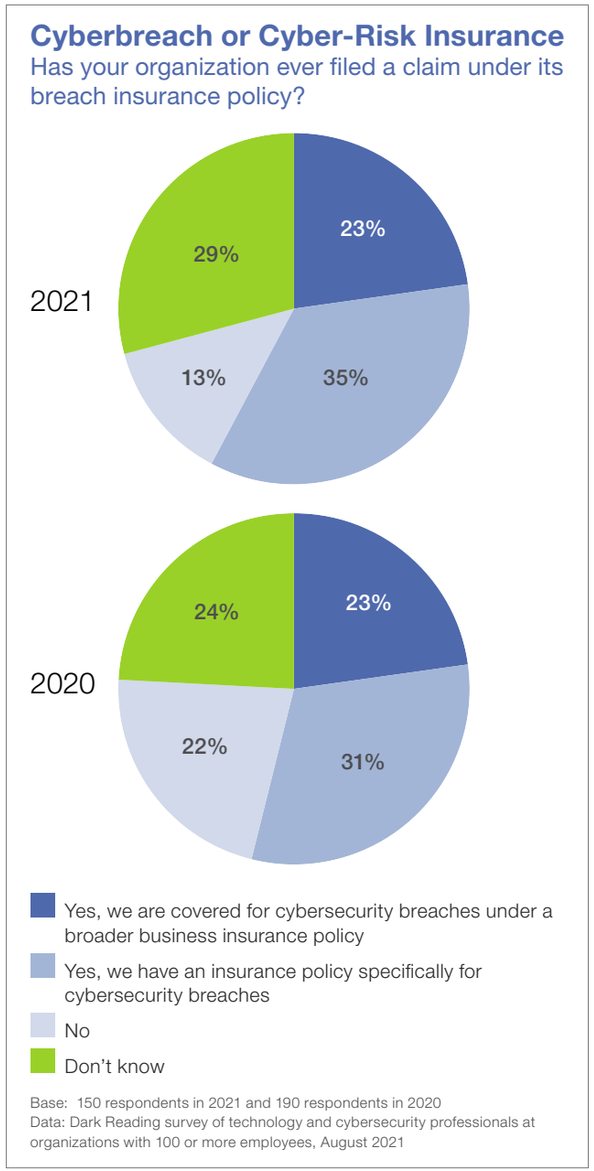


Figure 10.

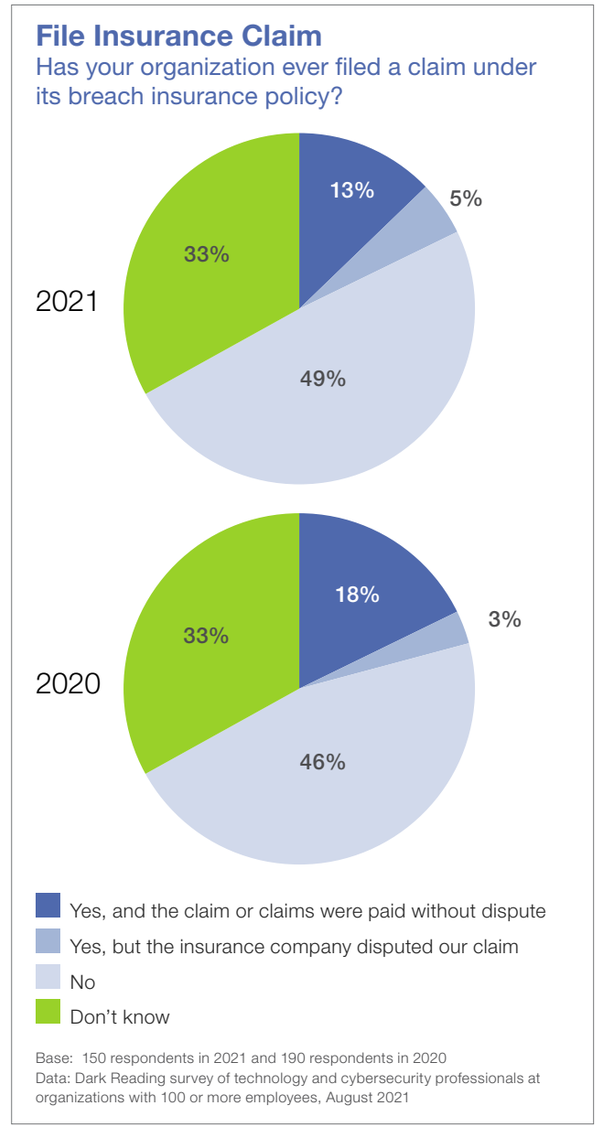
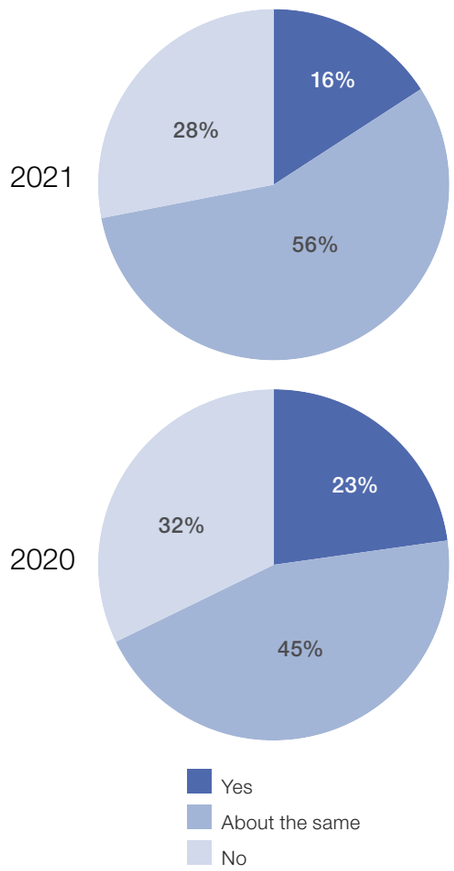


Figure 11.

Vulnerability to Security Breaches

Is your organization more vulnerable to security breaches than it was a year ago?

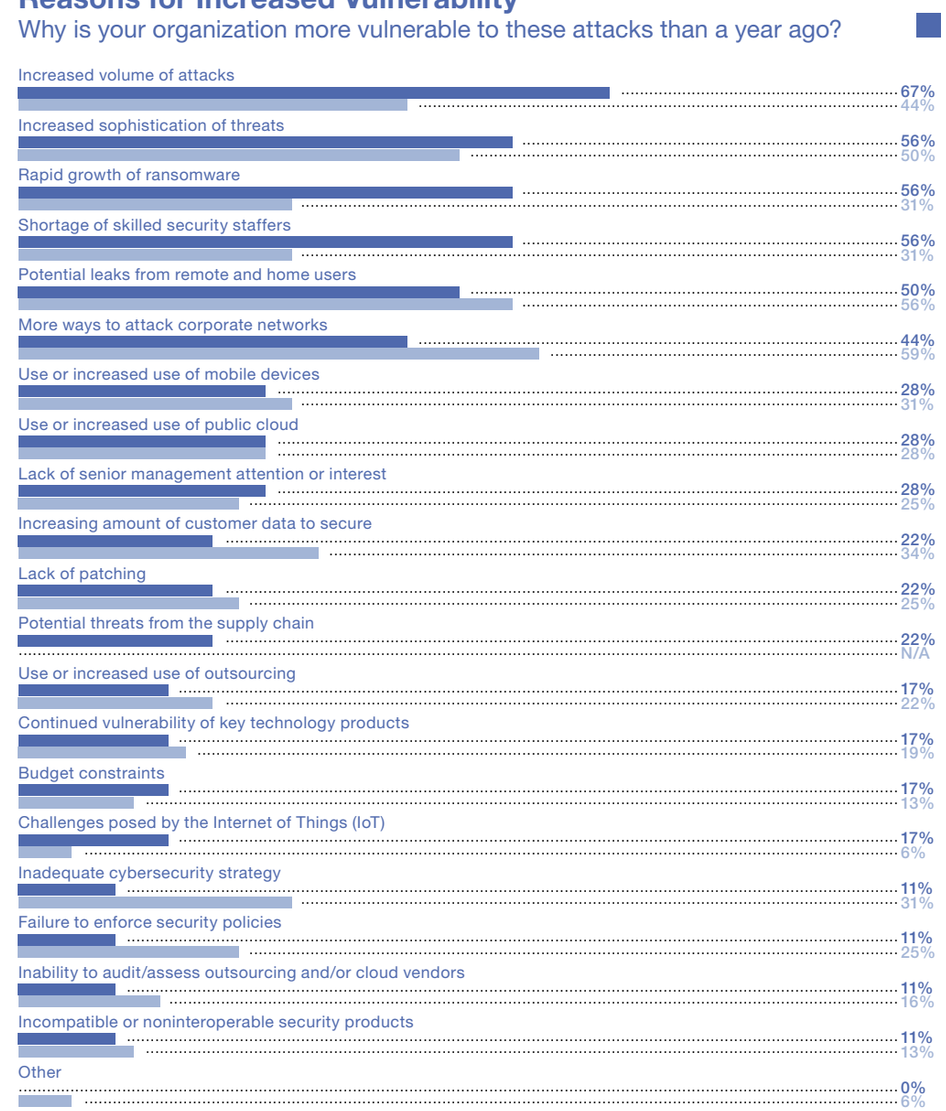


Base: 150 respondents in 2021 and 190 respondents in 2020
Data: Dark Reading survey of technology and cybersecurity professionals at organizations with 100 or more employees, August 2021

Figure 12.

Reasons for Increased Vulnerability

Why is your organization more vulnerable to these attacks than a year ago?



Note: Multiple responses allowed

Base: 24 respondents who are more vulnerable to attacks than a year ago in 2021 and 43 in 2020

Data: Dark Reading survey of technology and cybersecurity professionals at organizations with 100 or more employees, August 2021

respondents said their organizations were more vulnerable to a security breach because of potential data leaks from remote and home workers. This year, a smaller 50% identify this as a factor that has heightened their vulnerability exposure. Similarly, concerns over threat actors having a broader attack surface to target because of a distributed workforce have diminished significantly, with only 44% citing it as a reason for increased vulnerability, down from 59% a year ago.

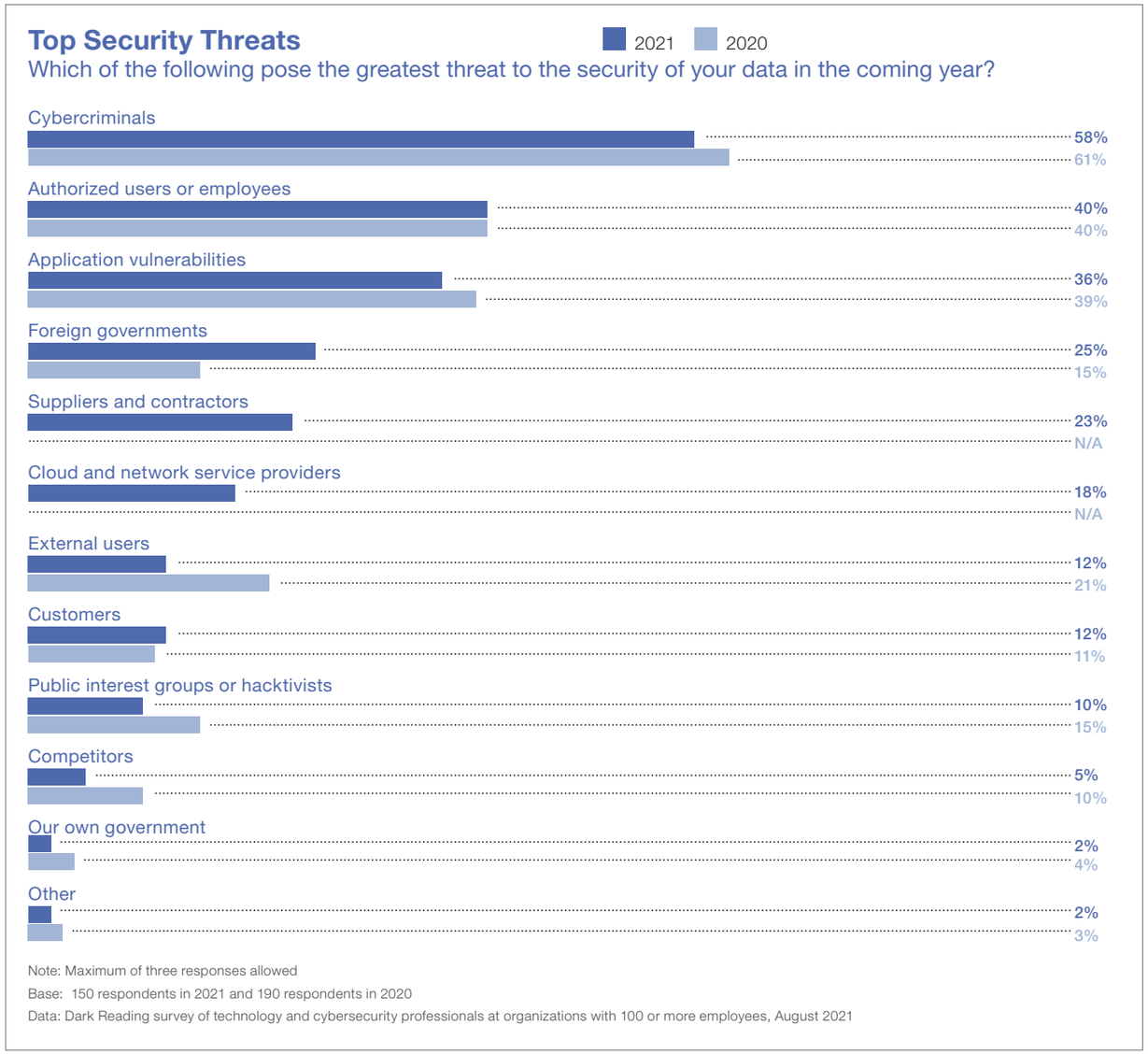
These and several other data points in Dark Reading's survey suggest that in the 18 months since the pandemic forced a shift to remote and home-based work, many organizations have gotten better at addressing new threats — or have a better understanding of threats — stemming from the transition. Last year, in the immediate chaos triggered by the shift to remote work, 38% described the devices used by home-based users as increasing enterprise risk. This year, just 25% say the same. Concerns over vulnerabilities in enterprise remote access systems and processes provided to work-from-home users have abated a bit as well, with 34% of respondents citing it as a source of increased enterprise risk, down from 39% last year.

Dark Reading's survey shows that while many IT and security leaders feel more confident in their ability to detect and respond to data breaches, they remain wary about a broad range of threats standing in their way. Topping their list of concerns, as it has for the previous two years, are cybercriminals and authorized users. Fifty-eight percent and 40% of survey takers, respectively, describe the two groups as posing the biggest threat to enterprise data **(Figure 13)**.

Concerns over the threat posed by authorized users are not new. But they have assumed greater significance with the move to a distributed work environment and the accelerated adoption of cloud services since the pandemic began in early 2020. The trend has made it harder for security teams to protect enterprise data and applications against negligent and careless users. It has also complicated the task of protecting against attackers using stolen user credentials to access enterprise data and systems. Concerns over the issue are driving interest in zero-trust security models, where every request to access enterprise assets is authenticated, regardless of whether the request is made from inside or outside the network. A report that Ericom Software released in September 2021 showed that more than 80% of organizations plan to at least begin implementing a zero-trust model within a year.

Other issues that respondents to our survey identify as major threats to enterprise data include application vulnerabilities (36%); foreign governments (25%); third-party suppliers and contractors (23%); and cloud and network service providers (18%).

Figure 13.



Conclusion

Organizations that experience a data breach are at heightened risk of network disruptions and application outages. Many can expect substantial financial losses, negative publicity, and brand damage after a data breach. Growing attack volumes and threat sophistication have resulted in a substantial number of organizations feeling more vulnerable to a breach compared with a year ago.

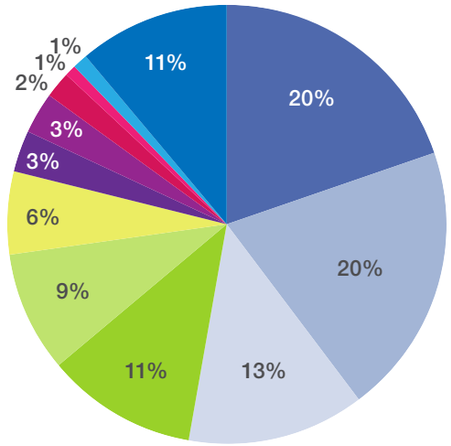
Many expect they will have to respond to a major breach in the next 12 months. Concerns are high over targeted attacks and the threat posed by state-backed actors, even though few organizations report an actual breach that involved either of these two causes. A handful of high-profile security incidents have elevated ransomware concerns, even though fewer organizations this year experienced an actual ransomware incident. A high percentage of IT and security professionals are confident about their capabilities for responding to a breach event or ransomware attack. However, they remain as wary of cybercriminals, users with authorized access to enterprise systems and data, app vulnerabilities, and third-party risk.

APPENDIX

Figure 14.

Respondent Job Title

Which of the following best describes your job title?



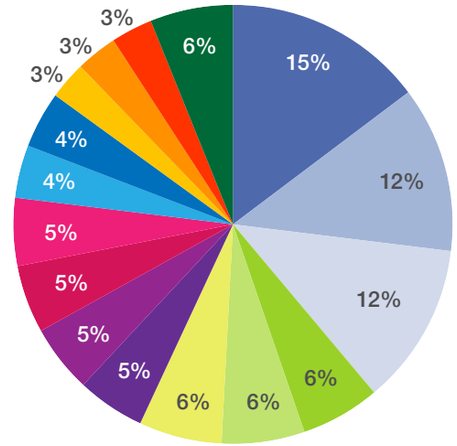
- IT director/head
- Information security department staff
- Information security director/head
- Information security department manager
- IT executive (CIO, CTO)
- Network/system administrator
- Non-IT/security director/VP
- Chief security officer
- Chief privacy officer
- Internal auditor
- President/CEO/managing director
- Other

Data: Dark Reading survey of 150 technology and cybersecurity professionals at organizations with 100 or more employees, August 2021

Figure 15.

Respondent Industry

What is your organization's primary industry?



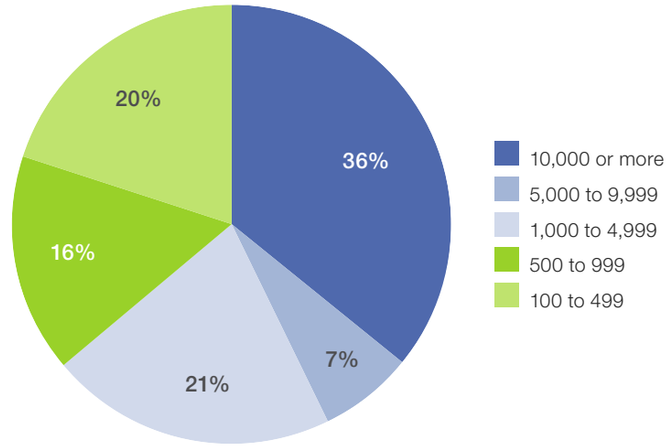
- Healthcare/pharmaceutical/biotech/ biomedical
- Banking/financial services/VC/accounting
- Government
- Communications carrier/service provider
- Computer or technology manufacturer/ tech vendor
- Solutions provider/VAR
- Aerospace
- Consulting/business services
- Media/marketing/advertising
- Wholesale/trade/distribution/retail
- Education
- Legal
- Insurance/HMOs
- Manufacturing & process (non-computer)
- Utilities
- Other

Data: Dark Reading survey of 150 technology and cybersecurity professionals at organizations with 100 or more employees, August 2021

Figure 16.

Respondent Company Size

Approximately how many employees are in your organization?

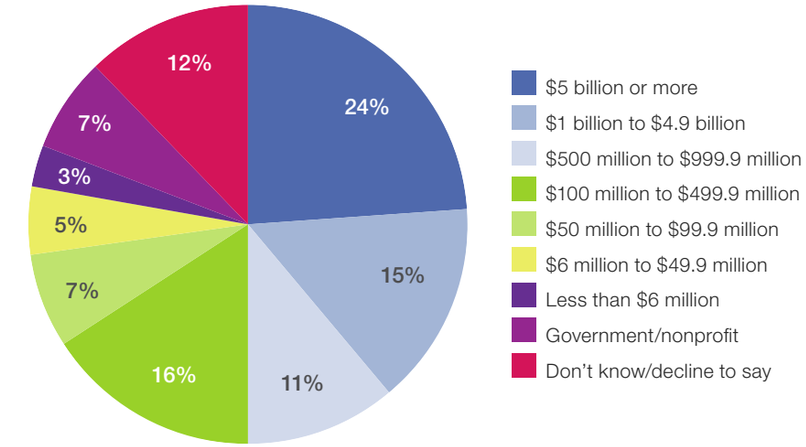


Data: Dark Reading survey of 150 technology and cybersecurity professionals at organizations with 100 or more employees, August 2021

Figure 17.

Respondent Company Revenue

What is the annual revenue of your entire organization?



Data: Dark Reading survey of 150 technology and cybersecurity professionals at organizations with 100 or more employees, August 2021