CISOs hurdle an extreme test of resilience, plan to emerge stronger

Digital Trust Insights Pulse Survey Findings 2020
Table of contents

Overview 3
Investments that paid off 4
Surge in attacks 9
Test in resilience 13
Rethinking cyber strategies 18
From war room to board room 23
Action plan for CISOs 26
About the survey 28
Demographics and business context 29
Contact us 33
Overview

PwC’s Digital Trust Insights Pulse Survey of 141 security and information leaders is akin to an after-action report on the first responses to the COVID-19 pandemic. How did they weather this extreme test of resilience? How are they rethinking their strategy and investments going forward?

The digital economy propped up the whole economy when businesses shuttered workplaces during the coronavirus outbreak. Tech firms and digitally native companies provided the backbone, while other businesses accelerated digitization — including automation, virtual collaboration, distributed work, cloud adoption, telehealth, direct-to-consumer channels, drone monitoring and 3D printing.

Boards and C-suite executives, who in the past may have wondered about the return on investment for all the cybersecurity personnel, solutions and architectures, don’t anymore. The value of their cybersecurity expenditures over the years — and of the CISO’s leadership — became crystal clear during this crisis.

Today, CISOs and CIOs are adjusting to a different future. All but two percent of CISOs/CIOs plan shifts in cyber strategy. They’re reprioritizing investments. Seventy percent expect their organization’s revenues to decrease in 2020 as a result of COVID-19; more than a quarter anticipate declines of more than 25%. It’s a once-in-a-lifetime kind of challenge. CISOs and CIOs must play a major role as businesses pursue twin goals in coming months: accelerating digital models and restoring organizations to financial health.

- CISOs and CIOs were on the frontlines as C-suite execs shaped crisis plans, especially the sudden shift to large-scale remote work and the acceleration of digitization in new or previously untested areas.
- They stayed in the war rooms, vigilant to outbreaks in cyber attacks that typically rise during crises.
- They remained focused on critical strategic projects, with a view toward building resilience against crises like this one.
- They pitched in on non-cyber projects, collaborating with risk, business, legal and tech leaders to protect and defend the organization from new risks.
Investments in the past two to three years that paid off the most during the crisis were not one-off security solutions.
Investments in the past two to three years that paid off the most during the crisis were not one-off security solutions.

CISOs surveyed said they invested in eight different areas, on average, over the past two to three years. The ones that paid off the most during the crisis were investments related to three capabilities. Critical to the sudden large-scale shift to remote work were investments such as VPN, VDI, mobile device management, endpoint security and identity-based network architecture. Helpful for crisis management were investments in resilience capabilities, such as business continuity and disaster recovery planning and managed detection and response services. Investments in data-driven risk management — such as real-time threat intelligence, use of data analytics and quantification of cyber risk — were also helpful as information evolved quickly during the crisis.

**Takeaway:**

Was making the right investments just a matter of good luck, or was it due to foresight? The answer lies beyond the scope of this Pulse Survey. But we know this from our 2019 Digital Trust Insights study on business-driven cybersecurity: Only about 25% of cybersecurity organizations had reframed their team’s mission to align with the company’s strategic goals. Business-driven cybersecurity leads to cyber investments that are more likely to yield tangible returns.
Within the past 2-3 years, which of the following areas has your company made significant investments in (e.g. upgrades, modernization or integration across the enterprise)?

Those with a Security Specific Job Role made an average of 8 investments in the past 2-3 years versus 6 for non-security roles

- Cloud Adoption: 40%
- Business Continuity or Disaster Recovery planning: 40%
- Virtual Private Network (VPN): 39%
- Move to identity-based network architecture (e.g. segmentation, Zero Trust): 21%
- Security awareness training and cross training security operations: 57%
- Managed security (MS): 33%
- Managed detect response (MDR) services: 33%
- Endpoint security solutions: 46%
- Access Management (e.g. Federation, SSO): 39%
- Modern mobile device management (MDM): 38%
- Real-time threat intelligence capabilities: 36%
- Virtualizing security operations center: 33%
- Virtual Desktop Infrastructure (VDI) product or solution: 31%
- Identity Governance and Compliance: 40%
- Third-party risk management processes: 39%
- Development of enterprise-wide information governance standards and frameworks: 38%
- Use of data analytics and AI in Cyber: 36%
- Global monitoring of privacy regulations and compliance: 34%
- Cyber analytics as part of overall ERM reporting: 33%
- Quantification of cyber risk: 33%
- None of the above: 1%

Source: PwC Digital Insights Pulse Survey, June 2020: base 141
Investments made in the past 2–3 years that have earned the highest marks in terms of positive impact during the crisis

What have been the impact of investments made in the past 2–3 years during the COVID-19 crisis to-date? (Respondents who say "significantly positive or positive" impact)

- VPN: 89%
- VDI: 86%
- Identity-based network architecture: 83%
- Modern mobile device management: 83%
- Endpoint security solutions: 78%
- Managed detection and response services: 91%
- Business continuity and disaster recovery planning: 79%
- Real-time threat intelligence: 86%
- Use of data analytics and AI: 86%
- Quantification of cyber risk: 85%

Source: PwC, Digital Trust Insights Pulse Survey, June 2020: base of 141, rounded results
Full breakdown of investments in the past two to three years that paid off

<table>
<thead>
<tr>
<th>Network/Infrastructure</th>
<th>People</th>
<th>Tech Solutions</th>
<th>Frameworks/Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud adoption</td>
<td>28%</td>
<td>44%</td>
<td></td>
</tr>
<tr>
<td>Business Continuity or Disaster Recovery planning</td>
<td>48%</td>
<td>30%</td>
<td></td>
</tr>
<tr>
<td>Virtual Private Network (VPN)</td>
<td>55%</td>
<td>35%</td>
<td></td>
</tr>
<tr>
<td>Move to identity-based network architecture (e.g.)</td>
<td>40%</td>
<td>43%</td>
<td></td>
</tr>
<tr>
<td>Security awareness training and cross training security</td>
<td>36%</td>
<td>43%</td>
<td></td>
</tr>
<tr>
<td>Managed security (MS)</td>
<td>36%</td>
<td>30%</td>
<td></td>
</tr>
<tr>
<td>Managed detect response (MDR) services</td>
<td>51%</td>
<td>40%</td>
<td></td>
</tr>
<tr>
<td>Endpoint security solutions</td>
<td>40%</td>
<td>38%</td>
<td></td>
</tr>
<tr>
<td>Access Management (e.g. Federation, SSO)</td>
<td>25%</td>
<td>47%</td>
<td></td>
</tr>
<tr>
<td>Modern mobile device management (MDM)</td>
<td>41%</td>
<td>43%</td>
<td></td>
</tr>
<tr>
<td>Real-time threat intelligence capabilities</td>
<td>53%</td>
<td>33%</td>
<td></td>
</tr>
<tr>
<td>Virtualizing security operations center</td>
<td>26%</td>
<td>43%</td>
<td></td>
</tr>
<tr>
<td>Virtual Desktop Infrastructure (VDI) product or solution</td>
<td>30%</td>
<td>48%</td>
<td></td>
</tr>
<tr>
<td>Identity Governance and Compliance</td>
<td>23%</td>
<td>50%</td>
<td></td>
</tr>
<tr>
<td>Third-party risk management processes</td>
<td>35%</td>
<td>42%</td>
<td></td>
</tr>
<tr>
<td>Development of enterprise-wide information governance</td>
<td>36%</td>
<td>40%</td>
<td></td>
</tr>
<tr>
<td>Use of data analytics and AI in Cyber</td>
<td>43%</td>
<td>43%</td>
<td></td>
</tr>
<tr>
<td>Global monitoring of privacy regulations and compliance</td>
<td>23%</td>
<td>46%</td>
<td></td>
</tr>
<tr>
<td>Cyber analytics as part of overall ERM reporting</td>
<td>32%</td>
<td>49%</td>
<td></td>
</tr>
<tr>
<td>Quantification of cyber risk</td>
<td>40%</td>
<td>45%</td>
<td></td>
</tr>
</tbody>
</table>

What has been the impact of these investments during the COVID-19 crisis to date?

Significantly positive

<table>
<thead>
<tr>
<th>Network/Infrastructure</th>
<th>People</th>
<th>Tech Solutions</th>
<th>Frameworks/Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud adoption</td>
<td>28%</td>
<td>44%</td>
<td></td>
</tr>
<tr>
<td>Business Continuity or Disaster Recovery planning</td>
<td>48%</td>
<td>30%</td>
<td></td>
</tr>
<tr>
<td>Virtual Private Network (VPN)</td>
<td>55%</td>
<td>35%</td>
<td></td>
</tr>
<tr>
<td>Move to identity-based network architecture (e.g.)</td>
<td>40%</td>
<td>43%</td>
<td></td>
</tr>
<tr>
<td>Security awareness training and cross training security</td>
<td>36%</td>
<td>43%</td>
<td></td>
</tr>
<tr>
<td>Managed security (MS)</td>
<td>36%</td>
<td>30%</td>
<td></td>
</tr>
<tr>
<td>Managed detect response (MDR) services</td>
<td>51%</td>
<td>40%</td>
<td></td>
</tr>
<tr>
<td>Endpoint security solutions</td>
<td>40%</td>
<td>38%</td>
<td></td>
</tr>
<tr>
<td>Access Management (e.g. Federation, SSO)</td>
<td>25%</td>
<td>47%</td>
<td></td>
</tr>
<tr>
<td>Modern mobile device management (MDM)</td>
<td>41%</td>
<td>43%</td>
<td></td>
</tr>
<tr>
<td>Real-time threat intelligence capabilities</td>
<td>53%</td>
<td>33%</td>
<td></td>
</tr>
<tr>
<td>Virtualizing security operations center</td>
<td>26%</td>
<td>43%</td>
<td></td>
</tr>
<tr>
<td>Virtual Desktop Infrastructure (VDI) product or solution</td>
<td>30%</td>
<td>48%</td>
<td></td>
</tr>
<tr>
<td>Identity Governance and Compliance</td>
<td>23%</td>
<td>50%</td>
<td></td>
</tr>
<tr>
<td>Third-party risk management processes</td>
<td>35%</td>
<td>42%</td>
<td></td>
</tr>
<tr>
<td>Development of enterprise-wide information governance</td>
<td>36%</td>
<td>40%</td>
<td></td>
</tr>
<tr>
<td>Use of data analytics and AI in Cyber</td>
<td>43%</td>
<td>43%</td>
<td></td>
</tr>
<tr>
<td>Global monitoring of privacy regulations and compliance</td>
<td>23%</td>
<td>46%</td>
<td></td>
</tr>
<tr>
<td>Cyber analytics as part of overall ERM reporting</td>
<td>32%</td>
<td>49%</td>
<td></td>
</tr>
<tr>
<td>Quantification of cyber risk</td>
<td>40%</td>
<td>45%</td>
<td></td>
</tr>
</tbody>
</table>

Source: PwC Digital Insights Pulse Survey, June 2020: base 141, nonrounded results
CISOs saw cyber attacks soar since February 2020 and expect threats to remain elevated in the next six months.
CISOs saw cyber attacks soar since February 2020 and expect threats to remain elevated in the next six months.

Cyber attacks increased in March and April, said more than half of the respondents, and about the same percentage expect an uptick in intrusions over the next six months. A phishing outbreak spread as the coronavirus and responses to it (the CARES Act, stimulus and relief programs) provided fresh, highly effective topical lures for business email compromise and social engineering campaigns. Remote work set-ups, accomplished quickly to enable business continuity, have brought increased exposure to threats. Attacks that were less prevalent — ransomware and denial-of-service attacks — show the largest increase in the number of survey respondents expecting rising risks through the end of 2020.

Cybercriminals, hackers and nation-state actors will continue to deploy proven techniques and invent new ones. Security analysts, investigators and incident responders, as well as penetration and vulnerability testers, will stay extremely busy responding to threat activity that will be elevated and will continue to evolve.

Takeaway:

Businesses demonstrated that they can quickly and smoothly shift their workforces from on-premise to remote. But many admit that they have much more to do to prove that their remote-work arrangements are secure.

The increase in distributed work — the mix of remote work, on-premise and managed services that’s here to stay — means that tests and security plans originally designed to protect perimeters are risky. With distributed work, the distinction between external and within-firewalls security protections has been erased.

Identity-based network architectures and Borderless Data Access Controls (BDAC) will help. BDAC asks “who, what, where, why and how” for every attempt — internal or external — to gain access to your critical data and infrastructure, and it authenticates relentlessly. Regardless of where the user or device is located, all face the same stringent scrutiny before accessing sensitive data. It’s consistent with a zero trust model: Trust isn’t freely given, but it must be earned. Everyone must pass the virtual “sniff test” every time, and continuously.
### A surge in COVID-19 related risks or attacks

**Within your company, have you seen a change in any of the following risks or attacks related to COVID-19, since February 2020?**

<table>
<thead>
<tr>
<th>Risk</th>
<th>Increase</th>
<th>No change</th>
<th>Decrease</th>
<th>Don't Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risks from use of non-enterprise devices and software (due to remote work)</td>
<td>62%</td>
<td>33%</td>
<td>5%</td>
<td>1%</td>
</tr>
<tr>
<td>Phishing attacks</td>
<td>61%</td>
<td>34%</td>
<td>5%</td>
<td>1%</td>
</tr>
<tr>
<td>Compliance and regulatory risks arising from moves to new models (e.g. telehealth, direct-to-consumer, etc.)</td>
<td>59%</td>
<td>33%</td>
<td>7%</td>
<td>1%</td>
</tr>
<tr>
<td>Risks coming through (inadequately secured) third parties</td>
<td>57%</td>
<td>37%</td>
<td>5%</td>
<td>1%</td>
</tr>
<tr>
<td>Access by non-credentialed users (due to remote work security gap)</td>
<td>51%</td>
<td>43%</td>
<td>5%</td>
<td>1%</td>
</tr>
<tr>
<td>Business email compromise</td>
<td>50%</td>
<td>45%</td>
<td>5%</td>
<td>1%</td>
</tr>
<tr>
<td>Ransomware</td>
<td>48%</td>
<td>40%</td>
<td>11%</td>
<td>1%</td>
</tr>
<tr>
<td>Denial of service attacks</td>
<td>40%</td>
<td>50%</td>
<td>9%</td>
<td>1%</td>
</tr>
<tr>
<td>Zero-day exploits</td>
<td>34%</td>
<td>57%</td>
<td>9%</td>
<td>1%</td>
</tr>
</tbody>
</table>

**And now looking ahead, in what way do you expect the incidence of COVID-19 related risks or attacks to change over the next 6 months?**

<table>
<thead>
<tr>
<th>Risk</th>
<th>Increase</th>
<th>No change</th>
<th>Decrease</th>
<th>Don't Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risks from use of non-enterprise devices and software (due to remote work)</td>
<td>61%</td>
<td>29%</td>
<td>10%</td>
<td>1%</td>
</tr>
<tr>
<td>Phishing attacks</td>
<td>61%</td>
<td>32%</td>
<td>7%</td>
<td>1%</td>
</tr>
<tr>
<td>Compliance and regulatory risks arising from moves to new models (e.g. telehealth, direct-to-consumer, etc.)</td>
<td>56%</td>
<td>35%</td>
<td>8%</td>
<td>1%</td>
</tr>
<tr>
<td>Risks coming through (inadequately secured) third parties</td>
<td>60%</td>
<td>32%</td>
<td>6%</td>
<td>2%</td>
</tr>
<tr>
<td>Access by non-credentialed users (due to remote work security gap)</td>
<td>49%</td>
<td>45%</td>
<td>6%</td>
<td>1%</td>
</tr>
<tr>
<td>Business email compromise</td>
<td>50%</td>
<td>48%</td>
<td>3%</td>
<td>1%</td>
</tr>
<tr>
<td>Ransomware</td>
<td>54%</td>
<td>36%</td>
<td>8%</td>
<td>2%</td>
</tr>
<tr>
<td>Denial of service attacks</td>
<td>48%</td>
<td>45%</td>
<td>8%</td>
<td>2%</td>
</tr>
<tr>
<td>Zero-day exploits</td>
<td>38%</td>
<td>46%</td>
<td>14%</td>
<td>2%</td>
</tr>
</tbody>
</table>

*Source: PwC Digital Insights Pulse Survey, June 2020: base 141*
Threat actor activity is expected to increase in the next 6 months

In what way do you expect threat actor activity from the following sources to change over the next 6 months?

<table>
<thead>
<tr>
<th>Source</th>
<th>Increase</th>
<th>No change</th>
<th>Decrease</th>
<th>Don’t Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybercriminals</td>
<td>72%</td>
<td>21%</td>
<td>7%</td>
<td></td>
</tr>
<tr>
<td>Hackers/hacktivists</td>
<td>58%</td>
<td>33%</td>
<td>9%</td>
<td>1%</td>
</tr>
<tr>
<td>Nation-state sponsors</td>
<td>52%</td>
<td>42%</td>
<td>4%</td>
<td>1%</td>
</tr>
<tr>
<td>Current employees</td>
<td>33%</td>
<td>51%</td>
<td>16%</td>
<td>1%</td>
</tr>
<tr>
<td>Past employees</td>
<td>24%</td>
<td>67%</td>
<td>9%</td>
<td>1%</td>
</tr>
</tbody>
</table>

Source: PwC Digital Insights Pulse Survey, June 2020: base 141
The pandemic called for CISOs to bring multifaceted capabilities to their job
The pandemic called for CISOs to bring multifaceted capabilities to their job.

During the pandemic, a CISO needed to be a tactical/operational CISO, as well as a transformational leader, a post-breach CISO, and a compliance and risk guru (four of the six types of CISOs described by Forrester Research). On average, nearly one-third of the CISO's time was allocated to crisis management, as expected. But nearly as much time was focused on business-as-usual operational tasks, and nearly one-fourth of their time was devoted to strategic cyber projects.

Half of the CISOs surveyed increased cybersecurity training and awareness for the full workforce, helping employees defend the organization from phishing attacks and remote-work-related risks. Slightly more CISOs increased cyber spending (35%) than reduced budgets (15%), but some adjusted staffing through furloughs (23%), headcount reduction (16%) or shifts to managed services providers (33%).

In the past, CISOs were often not included in strategic and business decisions and plans, even those with significant security and privacy implications. The pandemic may have changed all that. CISOs were significantly involved in decision-making around pandemic responses that were both operational and transformational: enabling remote work or work-from-home for the workforce (81%), setting up systems to monitor and report remote workers’ productivity (70%), planning for and coordinating return-to-work solutions for essential workers (71%), and implementing systems or apps to enable the monitoring of employee health and safety (65%).

Increased collaboration with business and risk functions during the crisis was reported by half of the CISOs, another sign of a turning point in CISO interactions.

Takeaway:

Crises precipitate new approaches; that’s how leading organizations emerge stronger from them. Greater integration with the business during this crisis is one such positive change that CISOs should sustain. Leading cyber teams bring greater value when they are connected on strategy, on a risk-based approach and in execution. They are twice as likely to work in strategic partnership with other functions that manage risk in their organizations and one-and-a-half times as likely to have a common understanding of how cyber risks fit within enterprise risk management.

CISOs have shown that business executives can be ambitious about the speed and scale of their digitization plans if they collaborate with their security and privacy chief from the start. It’s a way of operating that can also boost cyber teams’ professional satisfaction and purpose at work, and improve their ability to help their organizations. In a tight market for cybersecurity talent, two points that attract and retain talent are business leaders’ commitment to cybersecurity and CISOs who are actively engaged with the business, according to ESG ISSA’s 3rd annual survey.
The pandemic called for CISOs to bring multifaceted capabilities to their job.

During the crisis, how did you allocate your time in these activities? (Responses of 73 CISOs)

- 13% Non-cyber projects
- 25% Strategic cyber projects
- 29% Business-as-usual operational tasks
- 34% Crisis Management

CISOs took the following actions during the crisis:

- **Increased collaboration with other functions in the company**: 50%
- **Improved ability to conduct security operations remotely**: 36%
- **Real-time stress testing of resilience capabilities**: 24%
- **Increased training / awareness of cybersecurity across workforce**: 50%
- **Increased training on foundational cyber capabilities**: 37%
- **Increased cybersecurity spending / investments**: 35%
- **Deferred major cyber projects and investments**: 23%
- **Reduced the cybersecurity budget for the rest of the year**: 15%
- **Augmented our resources via managed services**: 33%
- **Changed cyber team full-time staffing (temporary furloughs)**: 23%
- **Reduced security team headcount (excluding furloughs)**: 16%
- **None at this time**: 4%

Source: PwC Digital Insights Pulse Survey, June 2020: base of 141
During the crisis, CISOs and CIOs managed the crisis and the ever present cyber threats, and kept strategic projects on track.

In terms of your time, during the crisis, how did you allocate your time in these activities?

- Non-cyber projects: 29%
- Strategic cyber projects: 24%
- Business-as-usual operational task: 15%
- Crisis management: 31%

In terms of your teams’ time, during the crisis, how did you allocate time in these activities?

- Non-cyber projects: 33%
- Strategic cyber projects: 22%
- Business-as-usual operational task: 30%
- Crisis management: 15%

Source: PwC Digital Insights Pulse Survey, June 2020: base 141
CISOs were significantly involved in decision-making, design and implementation of their organizations’ pandemic responses

With regard to the COVID-19 crisis, to what extent have you been involved in each of the following categories?

<table>
<thead>
<tr>
<th>Category</th>
<th>Decision making</th>
<th>Design</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling remote work or work-from-home for your workforce</td>
<td>81% 17% 1%</td>
<td>67% 30% 1%</td>
<td>61% 30% 9% 1%</td>
</tr>
<tr>
<td>Setting up additional controls/security for remote workforce</td>
<td>82% 15% 2%</td>
<td>70% 27% 1%</td>
<td>67% 25% 3% 2%</td>
</tr>
<tr>
<td>Setting up systems or apps to enable the monitoring of employee health and safety</td>
<td>65% 21% 10% 4%</td>
<td>47% 38% 9% 6%</td>
<td>57% 24% 13% 5%</td>
</tr>
<tr>
<td>Setting up systems to monitor and report remote workers’ productivity</td>
<td>70% 18% 6% 6%</td>
<td>60% 26% 7% 7%</td>
<td>60% 23% 9% 8%</td>
</tr>
<tr>
<td>Planning for and coordinating return-to-work solutions for essential workers</td>
<td>71% 25% 1%</td>
<td>65% 30% 1%</td>
<td>63% 28% 8% 1%</td>
</tr>
<tr>
<td>Coordinating alternate locations or remote work for security operations team</td>
<td>72% 21% 6%</td>
<td>68% 23% 6%</td>
<td>66% 22% 3% 6%</td>
</tr>
<tr>
<td>Leveraging 3rd party contractors to backfill security staff personally impacted by the virus</td>
<td>61% - 22% 14%</td>
<td>52% 29% 15%</td>
<td>55% 23% 8% 14%</td>
</tr>
<tr>
<td>Assessing the security of offshore vendors work-from-home solutions</td>
<td>68% 23% 6%</td>
<td>57% 30% 7% 6%</td>
<td>55% 30% 9% 5%</td>
</tr>
</tbody>
</table>

Source: PwC Digital Insights Pulse Survey, June 2020: base 141
The pandemic has induced CISOs to rethink their cyber strategy and investment priorities.
The pandemic has induced CISOs to rethink their cyber strategy and investment priorities.

Crises expose fragilities that are perennially ignored, hard to imagine or too costly to test. This pandemic was no exception. CISOs’ shifts in strategy and priorities are likely grounded in a better understanding of the extent of potential damage that could ensue if they don’t address certain specific gaps and vulnerabilities.

Topping the list of the most frequently mentioned changes in cyber strategy is ‘investing in better information governance standards and frameworks across their enterprise’ (39%). The absence — or patchwork state — of information governance would have been starkly evident to the CISOs as they had to quickly enable employees to work from home or move data to the cloud. They would have had to ask: What are our most critical assets? Where are they? And who has access to them?

Not surprisingly, ‘increasing resilience to severe events’ is another often-mentioned change in strategy (34%). Most organizations have much work to do to catch up to the top 25% of companies that scored well on three measures of resilience in our 2019 Digital Trust Insights study of resilient organizations: visibility into assets and interdependencies, defining and testing impact tolerances, and a set of capabilities that define “resilience by design.”

Takeaway:

About half of businesses don’t have an enterprise-wide information governance model (51%) or a common digital governance model (46%), according to our 2019 Digital Trust Insights study on business-driven cyber strategy. These are foundational models for organizations that want to increase cloud adoption or shift to digital operating models. Without these governance models in place, it will be difficult to realize desired cost savings or properly protect sensitive information. When in place, these models function as accelerators to help realize digitization plans and achieve returns.
Planned changes to cybersecurity strategy

Given what you learned during the crisis, which of the following are you prioritizing for future cyber investments to emerge stronger from the crisis?

Top ranked cyber strategy changes (indexed score)

<table>
<thead>
<tr>
<th>Change</th>
<th>Indexed Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invest in better information governance for better data-driven decision-making</td>
<td>100</td>
</tr>
<tr>
<td>Integrate cyber risks more with the overall enterprise risk management</td>
<td>95</td>
</tr>
<tr>
<td>Increase my company's resilience to severe events</td>
<td>92</td>
</tr>
<tr>
<td>Integrate better on business initiatives</td>
<td>79</td>
</tr>
<tr>
<td>Modernize the cyber infrastructure</td>
<td>78</td>
</tr>
<tr>
<td>Apply AI and other more advanced technologies in our work</td>
<td>76</td>
</tr>
<tr>
<td>Quantify cyber risks better</td>
<td>73</td>
</tr>
<tr>
<td>Automate more processes in the cyber function</td>
<td>65</td>
</tr>
<tr>
<td>Increase my team's digital skills</td>
<td>49</td>
</tr>
</tbody>
</table>

Source: PwC Digital Insights Pulse Survey, June 2020: base 141
How cyber investment priorities are shifting in the future, due to the pandemic experience

**Gaining in importance**
- Identity-based network architecture [e.g. segmentation, Zero Trust]
- Real-time threat intelligence capabilities
- Virtual desktop infrastructure (VDI) product or solution
- Development of enterprise-wide information governance standards and frameworks
- Managed Security (MS)
- Managed detection and response (MDR) services

**Remain important**
- Security awareness training and cross training security operations
- Business continuity or disaster recovery planning
- Cloud adoption
- Identity governance and compliance

**Getting less emphasis**
- Third-party risk management processes
- Endpoint security solutions
- Access management [e.g. Federation, SSO]
- Virtual private network (VPN)

Within the past 2-3 years, which of the following areas has your company made significant investments in?

Given what you learned during the crisis, which of the following are you prioritizing for future cyber investments to emerge stronger from the crisis?

Source: PwC Digital Insights Pulse Survey, June 2020: base 141
**Cyber investments prioritized for the future**

Given what you learned during the crisis, which of the following are you prioritizing for future cyber investments to emerge stronger from the crisis? (indexed score)

- **Move to identity-based network architecture (e.g. segmentation, Zero Trust)**: 100
- **Cloud Adoption**: 88
- **Business Continuity or Disaster Recovery planning**: 83
- **Virtual Private Network (VPN)**: 41
- **Security awareness training and cross training security operations**: 77
- **Managed detect response (MDR) services**: 68
- **Managed security**: 64
- **Real-time threat intelligence capabilities**: 79
- **Virtual Desktop Infrastructure (VDI) product or solution**: 74
- **Modern mobile device management (MDM)**: 62
- **Endpoint security solutions**: 50
- **Access Management (e.g. Federation, SSO)**: 44
- **Virtualizing security operations center**: 36
- **Development of enterprise-wide information governance standards and frameworks**: 62
- **Identity Governance and Compliance**: 59
- **Use of data analytics and AI in Cyber**: 56
- **Cyber analytics as part of overall ERM reporting**: 55
- **Global monitoring of privacy regulations and compliance**: 53
- **Third-party risk management processes**: 53
- **Quantification of cyber risk**: 53

Source: PwC Digital Insights Pulse Survey, June 2020; base 141
It’s time for imaginative and influential CISOs to step up
A majority of CISOs have interacted more frequently with their CEOs (65%) and the boards (50%) during the crisis. This trend points to a reset in CISOs’ interactions emerging from the crisis, and it should continue. In 2019, only 33% of all business and IT executives said that their cyber team communicates effectively with the board and senior executives about cyber risks and adjacent risks. But 71% in leading organizations (ones with business-driven cyber teams) report effective communications, according to that study on business-driven cybersecurity.

Effective communications with the board and CEOs requires many leadership skills that will be invaluable in the coming months.

The reopening of workplaces means new and different milestones for organizations to accomplish. CEOs are leading with an eye on both the pragmatic and urgent (how do I contain cost) and the new and long term (how do I apply tech to deliver better customer experience, and do things smarter and more efficiently) There’s repair to be done (how do I close security gaps in remote work setups) and a rethink-and-reconfigure to consider (what’s the office for when most of my employees can work in a distributed model).

This is the new arena where CIOs, CISOs and other business leaders will play in the next six months and beyond. A key question is, will cybersecurity and privacy be strategically woven into every consequential or bold move that corporate chiefs are contemplating?

CISOs love a good challenge. But can they do it under the toughest economic and financial situation in this lifetime? This is where imagination and influence will be required. What is the right cyber strategy to support their company’s reboot? What are the cyber priorities that can create competitive advantage for their company?

It’s time for imaginative and influential CISOs to step up.

In the 12 months prior to COVID-19 crisis, how often, if at all, did you interact with the CEO and the board?

<table>
<thead>
<tr>
<th>Frequency</th>
<th>The CEO</th>
<th>The Board</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily</td>
<td>13%</td>
<td>9%</td>
</tr>
<tr>
<td>Weekly</td>
<td>28%</td>
<td>18%</td>
</tr>
<tr>
<td>Bi-Monthly</td>
<td>19%</td>
<td>13%</td>
</tr>
<tr>
<td>Monthly</td>
<td>20%</td>
<td>18%</td>
</tr>
<tr>
<td>Quarterly</td>
<td>13%</td>
<td>32%</td>
</tr>
<tr>
<td>Every six months</td>
<td>1%</td>
<td>4%</td>
</tr>
<tr>
<td>Annually</td>
<td>2%</td>
<td>1%</td>
</tr>
<tr>
<td>No interaction</td>
<td>4%</td>
<td>3%</td>
</tr>
</tbody>
</table>

Source: PwC, Digital Trust Insights Pulse Survey, June 2020: base of 141
65% of CISOs say their interactions with the CEO have become more frequent during the crisis

In the 12 months prior to COVID-19 crisis, how often, if at all, did you interact with the CEO?

- Increased: 65%
- Unchanged: 28%
- Decreased: 4%
- Don’t know: 1%
- Not applicable: 2%

Source: PwC Digital Insights Pulse Survey, June 2020: base 141

50% of CISOs say their interactions with the board have become more frequent

In the 12 months prior to COVID-19 crisis, how often, if at all, did you interact with the board?

- Increased: 50%
- Unchanged: 36%
- Decreased: 7%
- Not applicable: 6%
- Don’t know: 1%

Source: PwC Digital Insights Pulse Survey Findings | 25
Action plan for CISOs
Action plan for CISOs

• Sustain the improved collaboration with the business and risk leaders beyond the crisis.

• Prioritize the identification and repair of any gaps or vulnerabilities that may have resulted from the crisis. Take the opportunity to modernize and simplify.

• Stay alongside the business to anticipate and manage risks that emerge from accelerated digitization, cloud adoption and shifts to digital business models.

• Continue to communicate frequently with the CEO and the board.

• Bring these leaders imaginative ways to improve security, resilience and trust, while helping to contain costs by being a good steward of the cybersecurity budget.
About the survey

Digital Trust Insights Pulse Survey 2020

This Digital Trust Insights Pulse Survey is a poll of 141 security and technology executives (CISOs, CIOs and similar titles) of US-based companies from May 8 to May 22, 2020. Sixty percent of respondents are executives in large companies ($1 billion and above in revenues); 13% are in companies with $10 billion or more in revenues. Respondents come from a range of industries: Tech, media, telecom (24%), Financial services (23%), Industrial manufacturing and automotive (19%), Consumer markets (17%), Health (12%), and Energy, utilities and mining (4%).

Comparable statistics are drawn from 2019 Digital Trust Insights studies conducted with more than 3,000 business and IT executives around the world.

The 2020 Global Digital Trust Insights, a survey of 3,000 business, security, risk, and tech executives around the world, will be conducted in July 2020.
Demographics and business context
141 US technology & IT leaders were surveyed in May to elicit their views on how cybersecurity and privacy strategies may change as a result of COVID-19

<table>
<thead>
<tr>
<th>Role</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Information Security Officer</td>
<td>49%</td>
</tr>
<tr>
<td>Head of IT</td>
<td>19%</td>
</tr>
<tr>
<td>Chief Information Officer</td>
<td>14%</td>
</tr>
<tr>
<td>Chief Technology Officer</td>
<td>14%</td>
</tr>
<tr>
<td>Chief Security Officer</td>
<td>2%</td>
</tr>
<tr>
<td>Head of Security</td>
<td>1%</td>
</tr>
</tbody>
</table>

**Company’s global revenue**

- **18%** US$250m to less than US$750m
- **50%** US$750m to less than US$2.5bn
- **18%** US$2.5bn to less than US$10bn
- **13%** US$10bn or greater

Source: PwC Digital Insights Pulse Survey, June 2020; base 141
Responses were achieved from a range of industries

Responses by sector

- TMT: 24%
- FS: 23%
- IM&A: 19%
- CM: 17%
- Health: 12%
- EUR: 4%

Responses by industry

- Technology: 21%
- Entertainment: 2%
- Communications: 1%
- Banking and Capital Markets: 10%
- Insurance: 8%
- Asset and Wealth Management: 6%
- Industrial Manufacturing: 13%
- Engineering & Construction: 4%
- Aerospace, Defense & Security: 3%
- Retail: 8%
- Transportation & Logistics: 4%
- Hospitality & Leisure: 2%
- Consumer Goods: 1%
- Forest, Paper & Packaging: 1%
- Healthcare: 10%
- Pharmaceuticals & Life Sciences: 2%
- Energy, incl. Oil & Gas: 3%
- Power & Utilities: 1%
- Other (Please specify): 1%

Source: PwC Digital Insights Pulse Survey, June 2020: base 141
The business context: 27% expect revenue declines greater than 25% in 2020 due to COVID-19

What impact do you expect on your company’s revenue this year, as a result of COVID-19?

- Decreased revenue by less than 10%: 9%
- Decreased revenue by 10%–24.9%: 29%
- Decreased revenue by 25%–49.9%: 18%
- Decreased revenue by more than 50%: 9%
- Decreased revenue of unknown magnitude: 5%
- We do not expect any impact to revenue: 6%
- Increased revenue: 10%
- It is difficult to assess at this point: 10%
- Don’t know: 4%

Source: PwC Digital Insights Pulse Survey, June 2020; base 141
Contact us

Sean Joyce
sean.joyce@us.pwc.com
Global and US Cybersecurity, Privacy and Forensics Leader, PwC US

Joe Nocera
joe.nocera@us.pwc.com
Cyber & Privacy Innovation Institute Leader, PwC US
Thank you