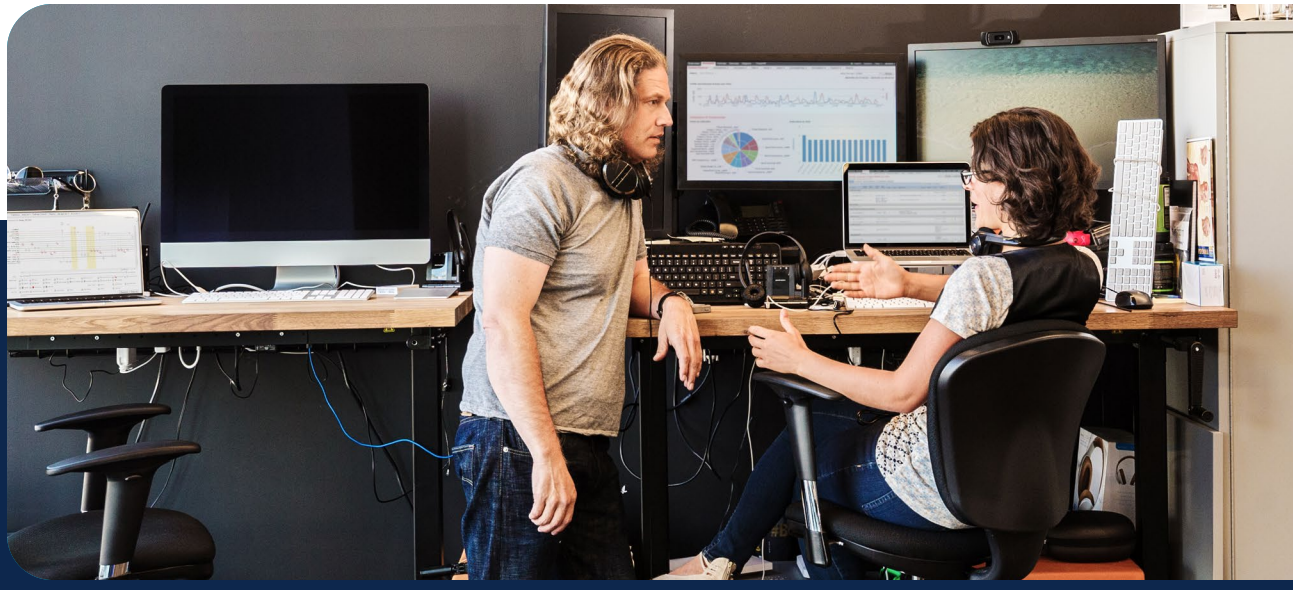
Secure your devices, connections, network, and data.

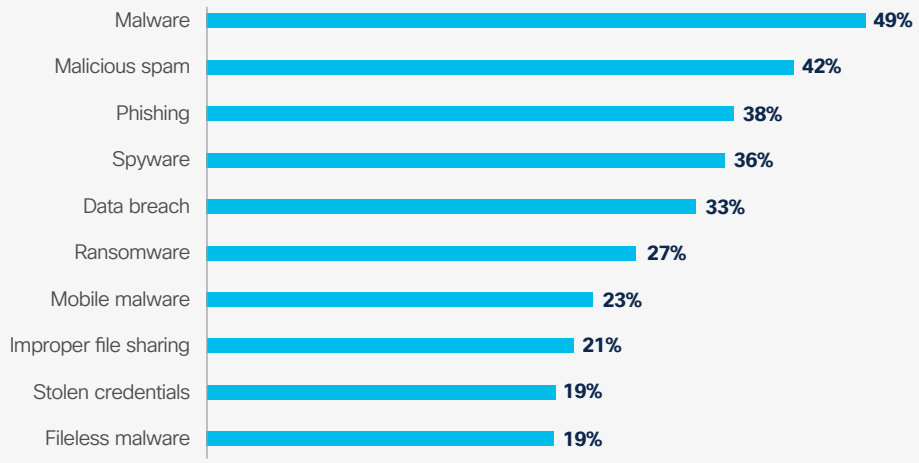


Cybersecurity should be a top priority for everyone who uses the Internet for business and personal activities. Protecting your assets encompasses an ever-expanding digital landscape. Globally, there will be 29.3 billion global networked devices, up from 18.4 billion connections in 2018 (source: *Cisco Annual Internet Report [2018-2023]*). More than half of those connections will support a wide variety of Internet of Things (IoT) applications (14.7 billion by 2023, compared to 6.1 billion in 2018). You need the actionable insights and scalable solutions to secure your employees' devices, IoT connections, infrastructure, and proprietary data. You also need the right partner to help you identify and remediate breaches quickly when unauthorized events occur.

Which security incidents and attack types have you encountered in the past year?

According to Cisco's 2019 chief information security officer benchmark study, two of the top three security issues pertain to email security. Whether you are investing in protecting the move to Microsoft Office 365 or trying to better protect against business email compromise (BEC) using Domain-based Message Authentication, Reporting & Conformance (DMARC), email remains the number-one threat vector. The fact that two of the top 10 attacks are insider threat issues (file sharing and stolen credentials) shows that you must look at what's happening inside as much as outside. Some criminals can log in rather than break in.

Top enterprise security issues



Source: *Anticipating the Unknowns: Chief Information Security Officer (CISO) Benchmark Study*, Cisco, March 2019.
[Percent of respondents: N = 2,909]

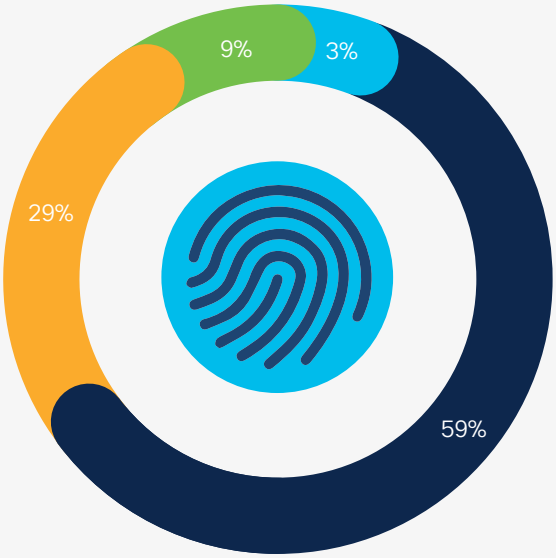
Recommended action

Today's security issues highlight the need for better multifactor authentication (MFA). Your security policy needs to strike the right balance between data protection and ease of use. An effective cybersecurity approach should give the right people access but not hinder authorized users with a clunky user authentication experience.

How well is your company complying with the current General Data Protection Regulation (GDPR)?

According to Cisco's 2019 data privacy benchmark study, 59 percent of global businesses indicated they meet all or most of the GDPR's requirements today. Another 29 percent said they will be GDPR ready within a year, leaving 9 percent who said it would take more than a year to get ready. While the GDPR applies to businesses in the EU or to the processing of personal data collected about individuals located in the EU, only 3 percent of respondents in the global survey indicated that they did not believe the GDPR applied to their organization.

GDPR compliance



- Currently meeting most/all of the GDPR requirements
- Not yet meeting most/all GDPR requirements, but we expect to within a year
- Not yet meeting most/all GDPR requirements, and it will take more than a year
- Not applicable—GDPR doesn't really apply to us

Source: *Maximizing the Value of Your Data Privacy Investments*, Cisco, January 2019.
[Percent of respondents: N = 3,206]

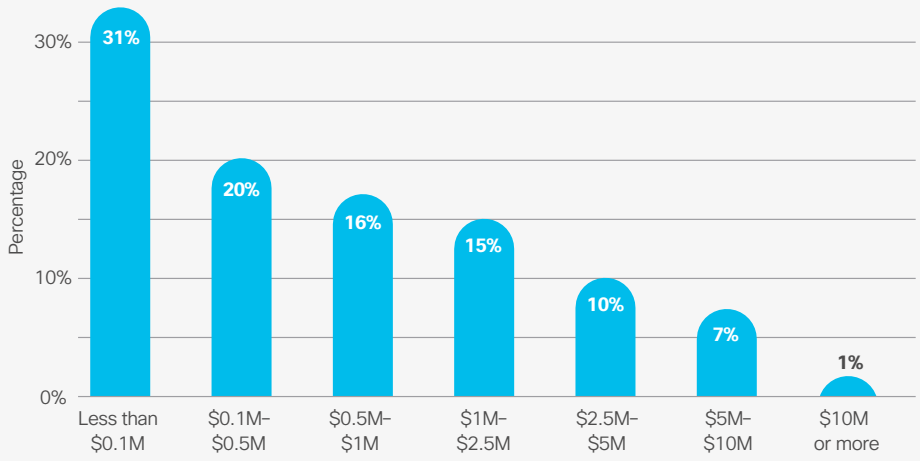
Recommended action

The top challenges to getting ready for the GDPR were identified as data security, employee training, and keeping up with the evolving regulations. Data privacy has become a board-level issue for many organizations, and customers are making sure their vendors and business partners have adequate answers to their privacy concerns before working together.

Over the past year, what was the financial impact of the biggest security breach to your organization?

We're all aware of the potential consequences of a breach: financial loss, brand and reputational setback or ruin, shaken stockholder confidence, loss of valuable data, regulatory and noncompliance penalties, and more. There is a clear shift toward issues of perception and sentiment. There's no let-up on the need to keep operations running, but customer experience and brand reputation are also key concerns related to cybersecurity issues.

Financial impact of a major security breach



Source: *Anticipating the Unknowns: Chief Information Security Officer (CISO) Benchmark Study*, Cisco, March 2019.
[Percent of respondents: N = 2,386]

Recommended action

All employees within an organization, especially those involved in security, should be extremely knowledgeable about incident response. Unfortunately, only 75 percent of Cisco survey respondents indicated that they knew what to do after a security breach. This is where training becomes so vital, and it needs to have greater prominence in every organization's cybersecurity plan.

Cisco can help you build and enhance a cybersecurity strategy and tactical plan.

Learn more from the *Cisco Annual Internet Report* >

- Learn more from the Cisco cybersecurity report series.
- Explore Cisco's comprehensive security solutions.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, see the Trademarks page on the Cisco website. Third-party trademarks mentioned are the property of their respective owners. The use of the word "partner" does not imply a partnership relationship between Cisco and any other company. (2004R)