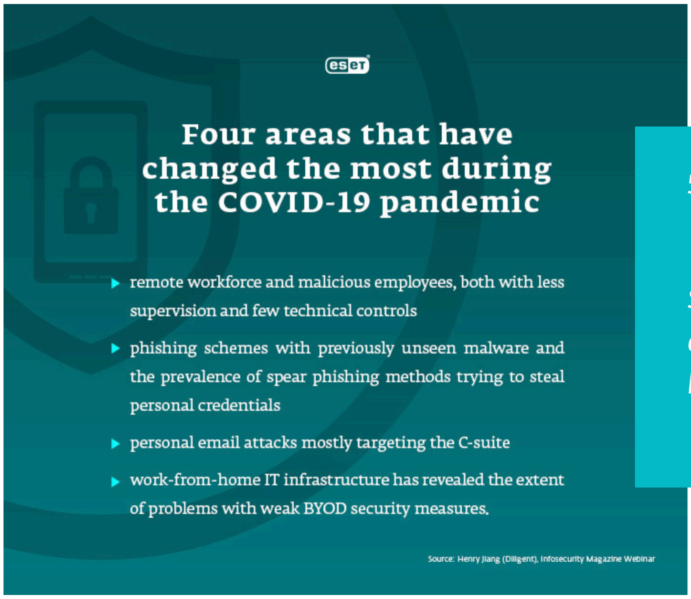
# How to get a budget for cybersecurity:

## Get inspired by the experts' approach

Without buy-in from executives, a lot of IT security experts have their hands somewhat tied. Fortunately, CEOs in general have become more concerned about cybersecurity over the past few years. Yet some of them still do not entirely grasp why IT security experts need more financial support. So, what can you do about it?



### Four areas that have changed the most during the COVID-19 pandemic

- remote workforce and malicious employees, both with less supervision and few technical controls
- phishing schemes with previously unseen malware and the prevalence of spear phishing methods trying to steal personal credentials
- personal email attacks mostly targeting the C-suite
- work-from-home IT infrastructure has revealed the extent of problems with weak BYOD security measures.

Source: Henry Jiang (Diligent), Infosecurity Magazine Webinar

Multiple points of view were shared by Infosecurity Magazine in their webinar, How to Win Budget & Buy-in from the C-Suite to Mitigate Increased Threats. It included a panel discussion about the current situation regarding investments in cybersecurity across companies. How has the cybersecurity landscape evolved since the start of the Covid-19 pandemic, and has the rise in cyberthreats fueled cybersecurity funding in companies all over the world?

*56% of companies in the US have dealt with a data breach.*

*—2021 Thales Data Threat Report*

*Stolen or compromised credentials were not only the most common cause of a data breach, but at 327 days, took the longest time to identify.*

*—IBM Cost of Data Breach report 2022*

One major theme is that many companies weren't prepared to secure personal devices when workers all around the world were forced to work remotely—and many still aren't, with no policies or guidelines in place. Mixing personal and business use of such devices represents one of the biggest current security challenges facing SMBs, for example, due to difficulties with segregating sensitive business data from an employee's personal email environment. Putting BYOD policies in place calls for creating an entire cybersecurity process of identifying and securing a personal device without intruding on private data (like GPS location or photos). This process can take months or even years to complete, requiring investments of both time and money.

BYOD stands for bring your own device and refers to employees using personal devices, such as smartphones, personal computers, or tablets to connect to an organization's network, accessing work-related systems and sensitive data. According to TechJury, 67% of employees use personal devices at work and 87% of businesses are dependent on their employees' ability to access mobile business apps from their smartphones, and the numbers are rapidly growing.

Although cybersecurity spending is reportedly growing, the lack of BYOD security measures is just one area that shows ample room for improvement. Two others are implementing cybersecurity training for all employees and building a cyber-aware business culture. All these improvements will likely involve **better funding and more top-level management involvement**. So how can you get your CEO on board?

## 1) Understand the environment in which you operate

As drivers for investing in cybersecurity vary—from the shift to a remote workforce to the increasing prevalence of ransomware—as a designated IT expert you need to clear up who you are trying to persuade and what their key concerns are. To do so, it may help you to engage across different teams to find out what their priorities are. When you make your case to the decision makers, be sure to address specific, relevant risk factors and explain how you plan to manage those risks.

## 2) Explain highly technical or oversimplified information about cyber risks

Your superiors should be aware of the current security situation in the company—and they often need to be coached through this discussion. **Everyone in the company must understand their responsibility**, but it always starts from the top. Business leaders may be following the news and reading up on cyber risks, but they may also lack the ability to translate that into company priorities and concrete measures. Instead, they might ask you yes-or-no questions like "Are we prepared for a ransomware attack?"

As an IT pro, it's up to you to clearly articulate security issues and explain where you see room for improvement. Help your CEO understand the probability of various types of incidents; research the security solutions that can help boost your defenses; and remind them that investing in stronger cyber protection benefits the bottom line.

## 3) Refrain from negative messaging

When talking about cybersecurity, IT managers often limit themselves to terrifying examples and worst-case scenarios. As ESET CISO Daniel Chromek stated in an interview, these tactics often fail as people will simply feel overwhelmed and adopt a defeatist mindset.  So when you're campaigning to get a boost in your cybersecurity budget, stick to the facts, provide practical solutions, emphasize the benefits, and you should be successful in your quest.

### Principles for driving a top-down approach in cybersecurity

1. Cybersecurity as a strategic risk
2. Legal and disclosure implications
3. Board oversight structure and access to expertise
4. An enterprise framework for managing cyber risk
5. Cybersecurity measurement and reporting

The top-down approach means that IT departments are not focused only on your company's tech stack while management is focused on the company mission and objectives, but they are interwoven and dependent on each other to ensure a well-secured work environment. It relies on continuous monitoring and protection of sensitive information.

Source: Diligent, Infosecurity Magazine, Opensource.com