The CISO’s Dilemma: Security Versus Productivity
Executive summary

Today organizations are struggling with the best way to protect against attacks that are targeting the endpoint. Too often, the security strategy has been to put the onus on the individual employee. Research has shown, over and over again, that training and user restrictions are both tedious and expensive, and have a very low success rate. This is because cybercriminals are experts at using social engineering to manipulate users into behaving insecurely.

This study looks at what today’s organizations are doing to prevent endpoint breaches targeting employees, the success of those efforts, and the associated costs that make this whole approach rather frustrating. We will also look at the impact that such measures have on productivity and ultimately the business’s ability to innovate.

We conclude by showing there is a different way to protect the endpoint. By allowing employees to work naturally – without restriction – we can still prevent malware from infiltrating the network. This approach has become a competitive advantage for our customers because it allows their employees to focus on innovation, not limitations. Users can ultimately click with confidence, knowing that any breach or attack will be isolated and prevented from entering the network.

About the research

This research is based on a survey of 500 CISOs from large enterprises across the USA (200), UK (200) and Germany (100) at organizations sized from 1,000 to 5,000+ employees. The research was carried out by Vanson Bourne, an independent market research organization.
Cybersecurity is a massive headache for organizations around the globe. According to the World Economic Forum, it is one of the top ten things keeping executives awake at night with CISOs reporting they’re now even more concerned about cybersecurity than they are about terrorist attacks.

The big question is ‘does the focus on security expose organizations to an even bigger risk: loss of market competitiveness?’ If we lock down users, prevent access to critical information sources, and tie them up in endless security training, we will hamper their ability to do their jobs effectively. So how do organizations balance security and productivity?

CISOs have rightly identified that employees are a key vulnerability, and they’ve responded by ramping up security education and training. This study reveals virtually all CISOs utilize a prohibition approach, limiting the risks by locking down employee access to certain external websites and restricting access to some applications. And it all comes at the cost of innovation, because limiting access means limiting creativity.

Prohibition doesn't work today. And it's even less likely to work in the future. Even after training...

Even after training and education, human beings are susceptible to manipulation via social engineering and are prone to making mistakes, leaving the organization exposed to risk. In fact, it’s not just mistakes: employees are being asked to assess risk vs. value every time they visit a webpage or open an email attachment. Right or wrong, they often determine the value of that activity to be more important than the potential risk.

But therein lies the rub: should employees be expected to make this judgement? Is it reasonable to expect people to know this difference between a legitimate business activity and the well-crafted deception conjured by a clever cybercriminal?

Digital organizations achieve agility through hyper-connectivity – both internally and externally – as well as by collaborating and co-developing ideas with customers, partners and sometimes even competitors. They also have flexible,
Global losses from security breaches, including lost productivity, are forecast to double from $3 trillion in 2015 to $6 trillion in 2021.

The current educate and prohibit approach is creating unsustainable tensions in the relationship between employees, the business, IT and security.

matrixed teams that work on a per-project basis, and such workforces utilize their own devices, applications and networks. Younger Generation Y and Z employees also see no reason not to Bring-Your-Own-Application and often simply ignore security restrictions to utilize tools that promise to make their jobs easier. More importantly, they may refuse to work for organizations that do not allow them free and unrestricted access to information and applications they wish to use.

Organizations that continue to rely on a prohibition approach to cybersecurity face an enormous loss of agility, innovation and productivity. This presents a huge dilemma for CISOs: how far do they go to protect their organizations against such losses?

The cost of security breaches and lost productivity is rising

The consequences are significant: global losses from security breaches, including lost productivity, are forecast to double from $3 trillion per year in 2015 to $6 trillion per year in 2021 according to analyst firm Cybersecurity Ventures. This report explains that the world’s attack surface is set to increase by an order of magnitude between 2016 and 2021, increasing global risk even further.

The report also highlights that the current educate and prohibit approach is creating unsustainable tensions in the relationship between employees, the business, IT and security. Employees are already complaining about the restrictions such policies place on their ability to get work done. In some cases, they are even going around security completely. And CISOs are being made to feel like the bad guys that always have to say no.

The current educate and prohibit approach isn’t effective, disrupts business, is unpopular with end users and doesn’t scale. There must be a way to deliver the required level of security without impacting productivity, innovation and collaboration.
Employees are the last line of defense against hackers

The idea that employees are the last line of defense in security is almost a cliché, because it’s true, end users are often the easiest target for hackers. In fact, the risk of employees unwittingly letting cybercriminals into IT systems continues to increase, as organizations – and employees – become more distributed and connected, continually expanding the attack surface.

According to IDC, 70% of security threats originate from the user endpoint. These attacks are becoming more sophisticated, with hackers utilizing a wide range of tactics to try and fool employees into making a mistake – whether that be spear-phishing, infected USB drives, insecure hotspots, man-in-the-middle attacks or polymorphic malware. Many attacks are based on social engineering – essentially asking humans to behave in a way that already comes naturally to them, i.e. clicking on a link or opening an attachment.

The best way to protect against these attacks – or so industry rationale goes – is to educate and train employees to be more aware of risks. We found this is a perspective shared by most CISOs according to our research, which revealed that virtually every CISO (99%) believes that user education, policies and procedures are essential to ensuring employees understand their role in keeping the business secure, as they are the last line of defense against hackers (Figure 1).

Figure 1: User education is essential to ensuring employees keep the business secure as they are the last line of defense

70% of security threats originate from the user endpoint according to IDC

74% of CISOs say employees have expressed frustration that security policies are hampering productivity

99% of CISOs believe that users are the last line of defense against hackers
This is true despite the evidence that social engineering was successful more than 43% of the time based on the 2017 Verizon DBIR. That means this viewpoint is not just talk: CISOs are also prepared to put their money where their mouth is. According to our research, 94% of CISOs have pushed for increased investment in user education following recent headlines around phishing and ransomware (Figure 2).

Figure 2: Greater awareness of phishing and ransomware is driving increased investment in user education

On the face of it, there is nothing wrong with the increased focus on user education, and it is good to have informed employees who are aware of cybersecurity issues – particularly, for instance, in preventing them falling into the trap of handing passwords over to social engineers. However, when you look closer, this education, alongside strict policies and procedures and restricted access to websites and applications, is leaving employees feeling exasperated.

Employees’ primary role is not one of security, yet they are being asked to think about security with nearly everything they do. In many cases their productivity is being harmed, as security restrictions or policies stop them doing what they need to. In fact, 74% of CISOs told us that employees in their organization had already expressed frustration at the way these policies were hampering their productivity (Figure 3).
One of the key reasons for their frustration is that in addition to education, many organizations are taking a hands-on approach to creating policies that restrict what end users can and can’t do on the endpoint. In fact, 88% of organizations restrict users from using websites and applications specifically because of security concerns (Figure 4). Furthermore, 94% have invested in web proxy services to help restrict what users can and can’t access (Figure 5).

© Bromium, Inc. 2017
Because of these restrictive measures, help desks and security teams are being deluged with complaints. Our research found on average, an organization gets complaints from users twice a week saying that legitimate work activity is being blocked or rejected by over-zealous security systems. Not only does this lead to a difficult relationship between security and the business, it also eats up the valuable time of security teams who are already pushed to the limit. On average 11 hours a week of IT, security and help desk time is spent fielding users’ complaints and requests for access to websites, applications and documents that have been blocked by security policies or tools (Figure 6).

Figure 6: Number of hours spent per week dealing with user requests due to access restrictions every week by IT, security and help desk teams
Employees see security as a barrier to innovation

In this context, it is no surprise that eight out of ten CISOs told us that they believe that employees see security as a barrier to innovation (Figure 7). Their frustration is understandable, particularly when you consider the number of people within an organization who are asked to open attachments from unknown third parties on a daily basis – it is nearly impossible to function without taking a security risk.

Security teams are well aware of employee frustration, which is accompanied by regular enquiries and complaints. Despite all their hard work, this means that security teams often feel unappreciated and misunderstood. More than three-quarters of CISOs (77%) told us they feel like they are now stuck in a Catch-22 situation, torn between keeping the organization secure and enabling innovation (Figure 8). Seven out of ten CISOs (71%) also said that they are personally made to feel like the bad guy by employees, because they are the ones that have to say no (Figure 9).

81% of CISOs believe employees see security as a barrier to innovation

77% of CISOs feel stuck trying to keep the organization secure while enabling innovation

It is nearly impossible to function without taking a security risk

© Bromium, Inc. 2017
The average employee spends seven hours per year on security training and learning processes.

HR, Legal, IT and Risk teams spend a further 276 hours per year on designing and delivering training.

For an organization with 2,000 employees, $290,033 is wasted each year on security training through lost productivity.

The cost of the educate and prohibit approach

So far we’ve reviewed the challenges to the educate and prohibit approach has on users, security teams and the organization at large. But what’s the cost?

To calculate the cost of employee security training and education, we asked CISOs how much time employees are spending on this in their organization. We found that the average employee now spends 7 hours per year in security training and learning processes (Figure 10). For an organization that employs 2,000 people this equates to a cost of $290,033 in terms of lost productivity.

Yet this is just one element of calculating the cost of user education. Added to this is time taken to design and deliver training, and create policies and procedures. The research revealed HR, Legal, IT and Risk teams spend on average 276 hours per year on this (Figure 11).

* $290,033 is calculated as follows: The average hourly pay of an employee is $21 based on data from the ONS in the UK, Statista in Germany, and the Department of Labor in the US. This was then multiplied by the 7 hours a year spent by individual employees on security education and training, and then multiplied by the average number of employees (2,000) in a large organization. The $290,033 figure doesn’t include the cost of hiring in external consultants to conduct training sessions with users, or the time spent by IT, legal and HR teams organizing internal sessions.
In addition to the time taken by internal staff, we also discovered that 90% of large organizations utilize external consultants to advise on and/or deliver education, training and policies (Figure 12). The average large organization employed consultants for 27 hours of work during the past year for these purposes.

Many businesses also support user education initiatives with stricter controls, enforced through technology. As mentioned previously, 94% of CISOs have invested in web proxy services to help restrict what users can and can’t access. The average cost for such solutions is just over $16 per user, per month: a total of $391,200 per year for an average organization of 2,000 employees (Figure 13).
The educate and prohibit approach to security acts as a ‘tax’ on business, frustrating employees and reducing productivity and innovation.

It’s time to let end users get back to work

If CISOs are to sleep soundly in their beds and drive the organization forward, it’s time for them to rethink the way they manage security risk. Alternative approaches exist to help minimize cybersecurity risks more effectively and in a scalable manner, which are far less restrictive on the business and its employees. The direct costs outlined in this report are only the tip of the iceberg. The indirect costs of prohibition are impossible to calculate, but probably dwarf the costs discussed in this research. Here’s just one simple example: what happens when a customer email is being continually blocked? The customer will go elsewhere.

There is also a correlated cost when employees take time away from their normal responsibilities to attend training. This associated cost is notoriously difficult to quantify, yet it exists. It’s hard for an organization to calculate the business value an employee could have generated if they hadn’t been pulled off their job for a day. But what’s even harder to quantify is the cost of employees being constrained in their daily tasks, because they aren’t permitted access, to websites or applications that would make them more productive or lead to additional business value.

Although these costs are hard to quantify, this report clearly shows that the educate and prohibit approach to security acts as a tax on business, frustrating employees and reducing productivity and innovation.
Eliminate the Catch-22

To resolve the dilemma of security versus productivity, organizations need to consider a new approach - one that protects their firm against risks, but also doesn’t have the enormous and costly impact of current educate and prohibit approaches.

This is exactly what Bromium does. Our unique application isolation and containment approach to security allows users to continue working, without even realizing they are doing so in a secure and separate environment. Using CPU-enforced micro-virtualization, tasks execute in a disposable, isolated virtual-machine (VM). Application isolation puts the activities most often targeted by cybercriminals – downloading files, using applications, browsing the internet – into micro virtual machines. When these activities are initiated, the network is protected because malware is trapped inside the container. As a result, restrictions on users can be lifted and employees can get back to work.

As such, organizations can:

- **Let freedom reign** - allow access to external websites and applications to support innovation, productivity and collaboration
- **Free up time** - enable employees to focus on doing their jobs instead of spending hours in education and training
- **Reduce overhead** - remove the expense of user education and training, third-party consultants, or restrictive technologies
- **Just say yes** - confidently remove restrictions and say yes to employee requests, by providing transparent security that supports business innovation


---

**ABOUT BROMIUM**

Bromium has transformed endpoint security with its revolutionary isolation technology to defeat cyber attacks. Unlike antivirus or other detection-based defenses, which can’t stop modern attacks, Bromium uses micro-virtualization to keep users secure while delivering significant cost savings by reducing and even eliminating false alerts, urgent patching, and remediation—transforming the traditional security life cycle.