Science.
Applied to Life.™

Whitepaper

Protecting your data

3 Reasons to Think Beyond Cybersecurity

We see it regularly: large-scale data breaches in the headlines. Today's organizations are constantly connected, making them vulnerable to cyber threats. To protect ourselves, we create robust cybersecurity plans that implement protective software and hardware — including firewalls, security architecture, and user controls. But data security goes beyond employing the right kinds of technology.

Here are three reasons to think beyond traditional cybersecurity measures when protecting your data:

1) The human factor

The most secure organizations know there's a human factor to data protection. In fact, failing to provide security training could negate the other efforts you've worked so hard to complete. According to Ponemon Institute, 25% of data breaches were caused by human error in 2015.[1] With an increasing number of technologies available to employees, and the ever-changing landscape of information security, it is critical that you train your people to handle, share, and protect data properly.

For example, social engineering is a known issue in the cyberworld. In their annual Internet Security Threat Report, Symantec found that spear-phishing campaigns targeting employees increased by 55% in 2015.[2] And it's not just the numbers that are increasing. The sophistication of phishing attempts is increasing too. As Symantec reports, "The social engineering involved in these phishing attacks is more sophisticated and targeted. They not only send generic scams… but seek to develop ongoing relationships, validate access to company information, and build trust."[3] With employees connected via many pathways — like email and apps — there are numerous ways for hackers to contact and coerce them into giving data away.

Mobile devices complicate security even further. Eighty-eight percent of employees admit to accessing confidential information on mobile devices — including email lists, customer data, financial information, and intellectual property.[4] This number raises questions about security, but when you add employees' handling of sensitive data, the situation becomes concerning. Sixty-six percent of respondents say they have downloaded and used unapproved apps for business, and 75% say their colleagues have put confidential information at risk — despite only 30% believing they have done so themselves.[5] Simply put, employees aren't clear on best practices when it comes to mobile security.

While the intent is not malicious, untrained employees present hackers with an easy job. For businesses, this means a security plan should include some component of education. Security awareness, good digital hygiene, and picking out a scam are skills that can — and should be — taught.

25%

of data breaches were caused by human error in 2015.[1]

2) The power of networking

Data leakage and security are not just issues for your IT team. Security efforts involve many areas of the organization, and a data breach can leave behind a myriad of damages — financial, operational, and reputational. With such vast effects, it's time that organizations used more resources and contacts to improve their security efforts.

Internally, more involvement from the Board of Directors will help. Traditionally, boards are concerned with the various risks an organization faces, and ensure that management has the right resources to minimize those risks. Given today's serious information threats, it's no wonder that boards are becoming more and more involved in cybersecurity efforts. According to PricewaterhouseCoopers (PwC), 45% of boards participated in overall security strategy in 2015 — and those organizations are seeing positive effects.[6] They saw a number of outcomes, including better identification of key risks, more alignment between cybersecurity efforts and overall business goals, and open communication between security teams and executives. Even better — these organizations had more money for security efforts, with a 24% boost in their security spending.[7] That's a significant increase, giving them more opportunity to protect their data.

Externally, organizations are sharing their threat intelligence. In 2015, 48% of businesses actively monitored or analyzed their security intelligence, and the number collaborating with others increased to 65%.[8] These organizations are reaping rewards for their openness. According to the Cost of a Data Breach study, breached organizations who participated in threat sharing incurred lower costs than their non-sharing counterparts.[9] With an expanding number of partners and customers, and an increasing amount of online data, the sharing trend is not surprising. Most say that external collaboration provides more actionable information from their industry peers, helping them improve their threat awareness and intelligence.[10]

And when it comes to security, knowing your weaknesses is half the battle. Today's hackers are experts at finding and exploiting security holes organizations don't even know they have. According to Symantec, attacks on these "zero day" vulnerabilities more than doubled in 2015.[11] Sharing weaknesses with your peers, or Information Sharing and Analysis Centres (ISACs), provides real-time insight that your internal teams cannot access alone.

In 2015

48%

of businesses actively monitored or analyzed their security intelligence

— and —

the number collaborating with others increased to

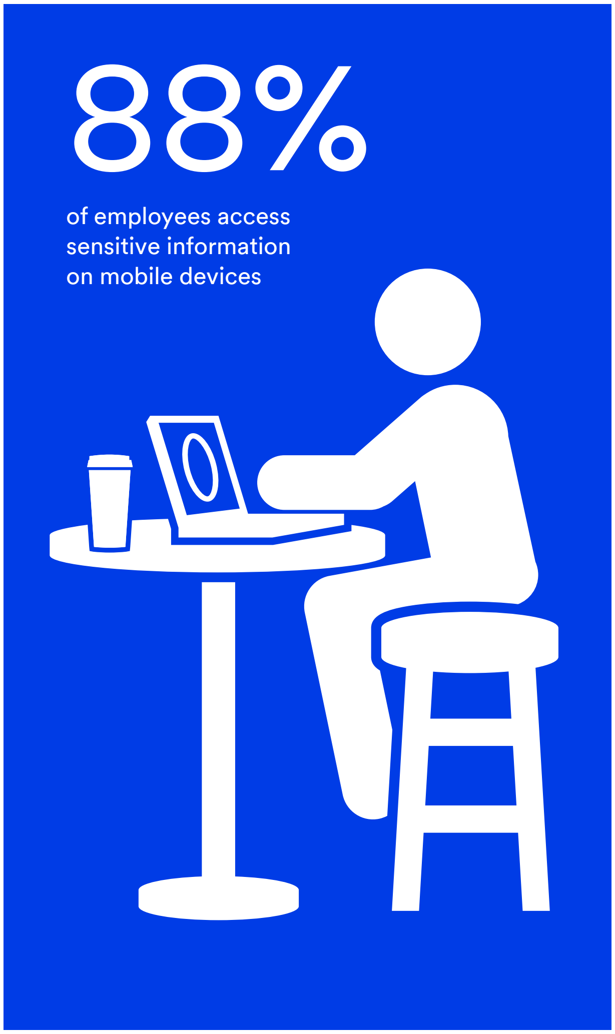
65%

3) The danger of low-tech hacking

Much of the time, your data is held within repositories, hard drives, or the cloud. It's tucked away, behind protective software. But it can't stay there forever. Your employees need that data to get their work done. And when they use it, your sensitive information is readily visible on-screen, where anyone can see it. Visual hacking — a low-tech method to capture sensitive, confidential, and private information for unauthorized use — is a growing concern. In a visual hacking experiment, a white hat hacker (a non-malicious person hired to help expose security vulnerabilities) successfully gleaned corporate information in 91% of instances.[12] This included sensitive information such as login credentials, classified documents, and financial information. Fifty-two percent of this sensitive information was captured from unprotected screens.[13] By simply looking over workers' shoulders, the white hat hacker achieved a data breach.

This study only focused on visual hacking within the office. Again, mobility makes your data security more complex. As stated previously, 88% of employees access sensitive information on mobile devices.[14] According to a Ponemon Institute survey, today's employees "have a growing dependency on mobile devices to access corporate information," and they are spending significant time working outside the office.[15] Whether it's during travel, in the office, or at a local coffee shop, our screens are viewable by everyone around us. With unprotected screens, mobile workers offer an easy opportunity for visual hackers to steal data.

When it comes to protecting on-screen data, one simple solution can make a world of difference: privacy filters. 3M Screen Privacy Products use advanced microlouver technology that blocks visibility from side views. Meanwhile, the intended user receives a crisp, clear view. Privacy filters, like those made by 3M, help to reduce the amount of data that can be visually hacked.[16]



88%

of employees access sensitive information on mobile devices

Enhance your cybersecurity plan

Today's organizations are extremely connected, with information stored and shared between numerous devices and users. Cybersecurity measures are undoubtedly important aspects of data protection. But that's not where it ends. Tactics that take place in the physical world — like implementing privacy filters, security training, and threat-intelligence sharing — can have a big impact on the security of your data. They have the power to prevent a full-fledged data breach. So you can protect your data now, instead of reacting after it's gone.

Without 3M™ Privacy Filters, your company's data is on show. Stay secure with 3M Privacy Filters for Monitors, Laptops, Tablets and Smartphones.

Find one that fits your organization at 3M.ca/Privacy

[1] Ponemon Institute, 2016 Cost of a Data Breach: Global Analysis, June 2016.
[2] Symantec, Internet Security Threat Report, Vol 21, April 2016.
[3] Ibid.
[4] Ponemon Institute, The Security Impact of Mobile Device Use by Employees, December 2014.
[5] Ibid.
[6] PwC, Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security® Survey, 2016.
[7] Ibid.
[8] Ibid.
[9] Ponemon Institute, 2016 Cost of a Data Breach: Global Analysis, June 2016.
[10] PwC, Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security® Survey, 2016.
[11] Symantec, Internet Security Threat Report, Vol 21, April 2016.
[12] Ponemon Institute, Global Visual Hacking Experiment, 2016, sponsored by 3M.
[13] Ibid.
[14] Ponemon Institute, The Security Impact of Mobile Device Use by Employees, December 2014.
[15] Ibid.
[16] Ponemon Institute, 3M Visual Hacking Experiment, 2015, sponsored by 3M and the Visual Privacy Advisory Council.

Privacy is the best policy.

3M