Infosys® | CONSULTING

WHY PEOPLE ARE THE WEAKEST LINK IN CYBERSECURITY

6 STEPS TO STRENGTHEN YOUR POLICIES POST COVID-19

An Infosys Consulting Perspective
By Ian Watts and Mick Burn

Consulting@Infosys.com | InfosysConsultingInsights.com

The Human Dimension

2020 will go down in history for many reasons, not least of which because it's the year most organizations were forced to leave their office buildings behind, and trust both technology and their employees to truly work remotely.

71% of employees access more company data, more frequently, from home now than they did pre-pandemic

Most companies managed the operational aspects of this change quite well, but there have been some challenges. According to data from security company Carbon Black, there was a 238% increase in the volume of global cyberattacks between February & April 2020.[1] This correlates with the shift to work from home globally and suggests that attackers are proactively targeting home workers

An IBM security report identified the average total cost of a data breach is $3.86 million in 2020, although the reputational damage is unquantifiable and more of a concern to many boards.[2] Remote working looks set to become a permanent way of life for many, so companies need to urgently investigate what is behind this rise in cybersecurity (CS) threats and take steps to mitigate it.

What has changed?

The pandemic changed the way people work almost overnight, without giving organizations the chance to update their technologies, policies, and staff training, and forcing some to take short-cuts to keep operations running.

90% of CS breaches are caused by human error rather than a system failure

In practice, working from home is often less secure than the office because workers use personal devices and insecure networks. HP research shows that “71% of employees access more company data, more frequently, from home now than they did pre-pandemic.”[3] When using a personal computer or laptop to access corporate data users are more exposed to cyberattacks. For example, employees may not have an antivirus or anti-malware installed or scan regularly. Additionally, a home office environment might not have enterprise level prevention and detection measures and are therefore much easier to attack.

Corporate tools like video conferencing services may also introduce new risks. According to a report from Deloitte, between February and May 2020 more than half a million people were affected by breaches in which the personal data of video conferencing services users (e.g., name, passwords, email addresses) were stolen and sold on the dark web.[4]

The common dominator within these trends is the human factor. According to the UK information commissioner’s office (ICO), 90% of CS breaches are caused by human error rather than a system failure.[5] The vast majority (almost 80%) of these are not malicious and are caused by the lack of awareness of CS threats, poor CS behaviours and not following procedures. However, an important point to mention is that even though these are not intended to harm organizations, the consequences caused by lack of CS controls and appropriate usage is same as of those classified as malicious: theft, elevation of access rights, destruction of information and illegal usage.[6]

Research suggests that 70% of people did not receive CS training leading to CS breaches, which correlates with the share of non-malicious attacks.[6] However, setting this issue aside, most professionals have a basic understanding of cybersecurity risks and their impacts, so why do they disregard CS training and practices? Are the training strategies not effective?

Between February and May 2020, more than half a million people were affected by videoconferencing breaches

What can organizations do?

Most organizations have already invested heavily in digital security technologies and associated processes. However, the level of understanding and maturity in cyber behaviors remains low. Infosys Consulting analysis suggests the reasons for the lack of compliance with cybersecurity policies is a combination of three factors:

1. Lacking a sense of personal accountability for cyber incidents
2. Busy workloads causing people to prioritize other immediate daily tasks taking the focus away from good CS practices
3. An assumption that CS breaches would not affect them: “will never happen to me” syndrome

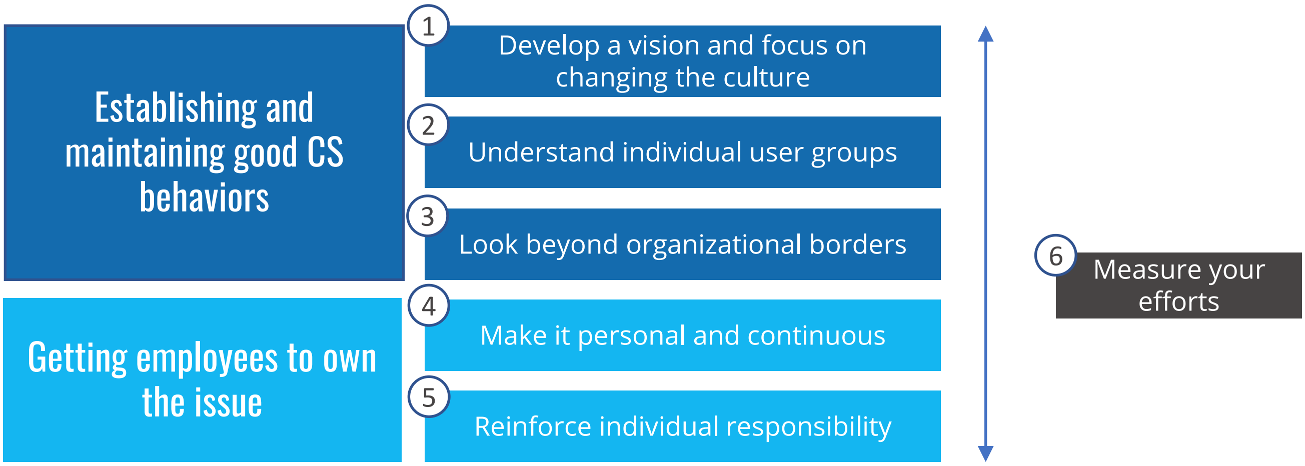
A comprehensive cybersecurity policy is a multi-dimensional combination of factors like technology and systems, effective and pragmatic policies, and processes and behaviors. These elements must be balanced within an organization. Most security functions focus on the first two and neglect the third. However, processes will not achieve the desired results if employees are not aware and do not have individual accountability – and technology will not provide security if employees bypass controls.

Corporates need to examine these behaviours and ask:

- Do individuals understand their personal role in cybersecurity?
- Is the cybersecurity function embraced by the employees?
- Are vulnerable groups recognized?
- Is there sufficient awareness and training?
- Is there a process to manage responsibility and accountability?

6 steps to strengthen your policies

The focus here should be on 6 steps that fall into two categories: 1. Establishing and maintaining good CS behaviors and 2. Getting employees to own the issue.


Establishing and maintaining good CS behaviors
Getting employees to own the issue
1 Develop a vision and focus on changing the culture
2 Understand individual user groups
3 Look beyond organizational borders
4 Make it personal and continuous
5 Reinforce individual responsibility
6 Measure your efforts

1. Develop a clear vision & focus on changing the culture

The first step of reinforcing your cybersecurity measures is understanding the “as is” status – particularly in terms of attitudes towards CS and pain points through focus groups, interviews, and surveys. Following this, leaders should focus on defining desirable behaviours to embed good practice within the culture.

Fundamental to this cultural shift is developing a clear vision for success, backed by leadership involvement and visibility. Recognising and celebrating good behaviors should be a top-down initiative and could include highlighting examples of best practice in company wide meetings, developing cybersecurity scorecards, and through financial based incentives.

2. Understand individual user groups

When carrying out an impact assessment, focus on how your employees use technology and how the current CS strategy fits with their existing processes. This means understanding sensitivity of the information used and types of technology and risks. It is also important to identify the level of vulnerability though their data access, usage lenses and differences in behaviours. The latter should include understanding how different employee groups are best engaged and their key concerns and safeguards - this can be achieved through design thinking workshops and persona definitions.

3. Look beyond the organizational borders

Good CS behaviours should cover how employees engage with third parties and other stakeholders. With the shift to working from home, organizational borders are inevitability blurring with personal life. Therefore, education on CS behaviours should be extended to family members, especially in the areas of online threats, password management, latest CS trends and best practices. Involving family members and changing individual behaviours is likely to reduce the pressure that working from home has on increasing the risk and exposure to CS threats at the organizational level.

4. Make it personal and continuous

Make it personal and continuous. Once risk areas and most vulnerable groups are identified, the focus should be on getting employees onboard and owning the issue. Specifically:

- Making training relatable and tailored to the audience.
- Developing an understanding of why CS is important for everyone.
- Making training digestible and understandable – this can be done in the form of gamification and short videos demonstrating CS challenges, which tend to be more effective than lengthy paper manuals.
- Keeping the content current – we recommend updating your employees on new sophisticated social engineering, phishing and cyberespionage and best practices related to home office devices, such as IoT devices, routers and printers, and corporate device usage. Importantly, this should be continuous process and not a one-off event.

5. Reinforce individual responsibility

While training will educate your employees on how to treat CS, without reinforcement and accountability, the desired results will not be achieved. Accountability should be implemented at each level; individuals must understand the consequences of not following good CS practices, not only at the organizational level but also at an individual level. For the team leads and managers, accountability needs to be translated into performance KPIs and become integral to meeting agendas.

6. Measure your efforts

Finally, it is also critical to measure your cybersecurity efforts. There are 3 key considerations here:

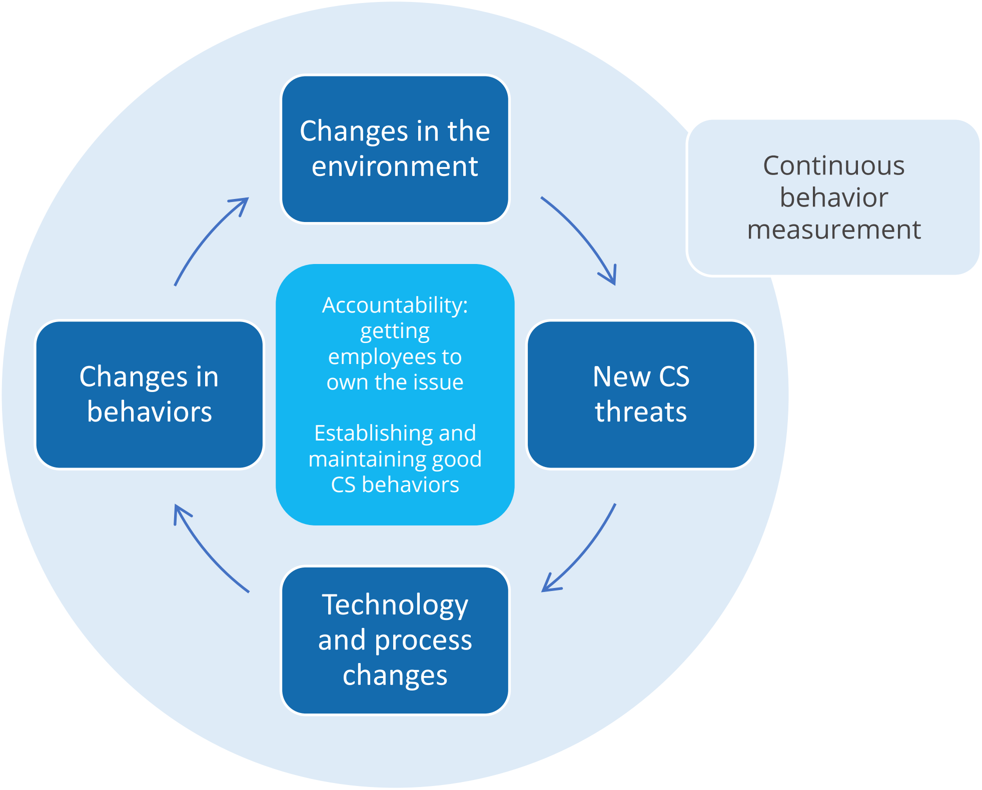
1. Metrics: Consider different metrics, such as how many phishing emails were opened, training scores, focus groups and interview data on CS awareness. Additionally, it is important to distinguish between user groups and identify the most vulnerable areas.
2. Usage of data: Dashboards and reports should become the norm for capturing and tracking CS behaviours over time. These should also measure the effectiveness of training programmes, which can be simply compared by assessing the metrics prior and post any campaigns.
3. Engage with the employees: We recommend replaying the results to the employees, highlighting most vulnerable areas and risks. Interviews, surveys, and feedback on employee CS awareness should become a regular and expected process.

Our Approach

At Infosys Consulting, we take a holistic approach to cybersecurity – ensuring that organizational change is embedded at the core of all security initiatives.

Figure 1 outlines how we work with clients to ensure that their policies are a multi-dimensional combination of technology and systems, effective and pragmatic policies, and processes and behaviors – to maintain a constant culture of good cybersecurity.

Maintaining good cybersecurity culture



Changes in the environment

New CS threats

Technology and process changes

Changes in behaviors

Accountability: getting employees to own the issue

Establishing and maintaining good CS behaviors

Continuous behavior measurement

There is no doubt that as businesses continue to grapple with the long-term impact of Covid-19, bad actors will continue to find vulnerabilities in security systems.

Even with the right staffing model and tools, people, not technology, are often at the heart of breaches. And the common denominator of many of the incidents we've supported clients on has been cultural – firms either failed to take risks seriously or acted as if cybersecurity was solely the responsibility of IT instead of fully integrating the topic within the business.

Looking to the future, it is helpful to remember that culture is shaped by executive action. For this reason, it is vital for cybersecurity to be included in both the dialogue and actions of C-level executives, providing a natural way for employees to understand that security is a company priority.

For discussion on how you can support your organization, get in touch with our experts.

MEET THE EXPERTS

Ian Watts

Partner, CIO Advisory

Ian.Watts@infosysconsulting.com

Mick Burn

Partner, Talent & Organization

Michael_Burn@infosysconsulting.com

Jaiprasad Mallepat

Principal, CIO Advisory

Jaiprasad.Mallepat@infosysconsulting.com

Sandra Sidlauskaite

Senior Consultant, Talent & Organization

Sandra.Sidlauskaite@infosysconsulting.com

References

1. VMware Carbon Black. (2020) Modern Bank Heists 3.0 available at: https://cdn.www.carbonblack.com/wp-content/uploads/VMWCB-Report-Modern-Bank-Heists-2020.pdf (Accessed: 1st July 2021).
2. IBM Security. (2020) Cost of a Data Breach Report available at: https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf/ (Accessed: 1st July 2021).
3. HP Wolf Security. (2020) HP Wolf Security Study Reveals Growing Cyber Security Risk Driven by Remote Work available at: https://press.hp.com/us/en/press-releases/2021/hp-wolf-security-study-risk-remote-work.html/ (Accessed: 1st July 2021).
4. Deloitte. (2020) Cyber crime – the risks of working from home available at: https://www2.deloitte.com/ch/en/pages/risk/articles/covid-19-cyber-crime-working-from-home.html (Accessed: 1st July 2021).
5. 90% of UK Data Breaches Due to Human Error in 2019 available at: https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/ (Accessed: 6th July 2021).
6. IT Governance UK. (2016) Accidental or malicious insider threat: staff awareness makes the difference available at: https://www.itgovernance.co.uk/blog/accidental-or-malicious-insider-threat-staff-awareness-makes-the-difference (Accessed: 1st July 2021).
7. AT&T Communications. (2021) Survey Suggests the Behaviour of Remote Workers is Adding Extra Cybersecurity Risk to Their Employers' Business available at: https://about.att.com/story/2021/att_cybersecurity_survey.html/ (Accessed: 1st July 2021).
8. CyberSecurity Insiders. (2020) Remote Work From Home CyberSecurity Report available at: https://rs.ivanti.com/reports/ivi-2537-wfh-cyber-security-report.pdf?psredirect/ (Accessed: 1st July 2021).
9. MounaJouinia, Latifa Ben ArfaRabaia, Anis BenAissab. (2014) Classification of Security Threats in Information Systems available at: https://www.sciencedirect.com/science/article/pii/S1877050914006528 (Accessed: 1st July 2021).
10. Brian Prince. (2015) Employees Not Following Policy is the Biggest Threat to Endpoint Security, IT Pros Say available at: https://www.securityweek.com/employees-not-following-policy-biggest-threat-endpoint-security-it-pros-say (Accessed: 1st July 2021).

Infosys® | CONSULTING

consulting@Infosys.com
InfosysConsultingInsights.com

LinkedIn: /company/infosysconsulting
Twitter: @infosysconsltng

About Infosys Consulting

Infosys Consulting is a global management consulting firm helping some of the world's most recognizable brands transform and innovate. Our consultants are industry experts that lead complex change agendas driven by disruptive technology. With offices in 20 countries and backed by the power of the global Infosys brand, our teams help the C-suite navigate today's digital landscape to win market share and create shareholder value for lasting competitive advantage. To see our ideas in action, or to join a new type of consulting firm, visit us at www.InfosysConsultingInsights.com.

For more information, contact consulting@infosys.com