

CYBERSECURITY CULTURE

What It Is, How It Works, and Why You
Need It In Your Organisation



 **K7 SECURITY**

Contents

- Introduction 3
- How Human Error Impacts Cybersecurity..... 4
- The Consequences of a Cyberattack 4
 - Direct Financial Costs 4
 - Indirect Financial Costs..... 4
 - Real-world Consequences 5
- Culture as a Defence Against Error 6
 - What Is, and Isn't, Culture..... 6
- Building a Culture of Cybersecurity 7
 - Hiring 7
 - Training 8
 - Procurement..... 9
 - Scrappage 9
 - Design 9
 - Partnerships 9
- Judging the Effectiveness of Cybersecurity Culture 10
- K7 Enterprise Cybersecurity 11



Introduction

All organisations like to develop an organisational culture around desirable traits e.g., developing a sales culture or a learning culture, because they need individuals to take the right decisions and perform the right actions without seeking guidance for every choice that presents itself. This reduces the need for micromanagement and allows the organisation to grow without compromising stability or having a top-heavy hierarchy.

Cybersecurity may not seem like an obvious candidate for a cultural trait as it is not perceived as a core function of the organisation. The need for a cybersecurity culture is often not apparent because it is seen as a technology problem that requires a technology solution, and cybersecurity solutions function in the background and are usually noticed only if they hamper operations or do not work correctly.

Cybersecurity that hampers operations can be avoided by choosing cybersecurity solutions that are known for not consuming IT resources, whether in the form of hardware resources, bandwidth, or the time and energy of the IT team. But cybersecurity solutions may fail to protect the organisation due to the actions of end users, and that risk is addressed by creating a culture of cybersecurity.





How Human Error Impacts Cybersecurity

We can understand the impact that human error or fallibility has on cybersecurity by considering these statistics:

- [22% of breaches](#) are caused by human error
- [37% of credential theft breaches](#) use stolen or weak credentials
- Phishing (a form of social engineering) accounts for [91% of cyberattacks](#)

The very large number of threats that depend on, or are the result of, user action (or inaction) indicate that the human element is a critical link in the cybersecurity chain and should not be ignored.

The Consequences of a Cyberattack

Some cyberattacks are just pranks that are more annoying than harmful, but many are intended to wreak havoc and have a significant impact on the top line and bottom line of a business. Costs incurred due to a cyberattack include:

Direct Financial Costs

Direct financial costs are usually incurred immediately after the attack, and can be directly linked to the attack.

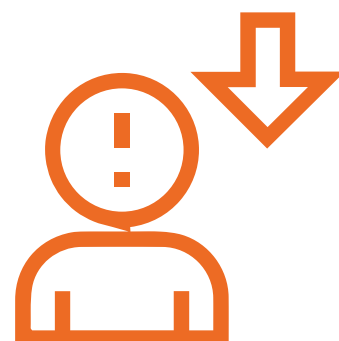
- **Operating Costs** – Attack remediation costs, such as consulting fees to IT specialists, legal and other compliance costs to manage regulatory impact, and marketing costs to avoid brand deterioration, can cause an increase in operating expenditure
- **Capital Expenditure** – Investment in enhanced cybersecurity measures and replacement of affected or vulnerable infrastructure can increase capital outlay
- **Opportunity Cost** – Money that is spent on recovering from the cyberattack is money that is not spent on other projects. Destruction or theft of Intellectual Property (IP) prevents monetisation of IP. Both of these can affect the growth of the business

Indirect Financial Costs

Indirect financial costs are the costs that are incurred some time after a cyberattack, may not be directly linked to the cyberattack, and may be in the form of lost income rather than additional expenditure.

- **Reputation Loss** – Disruption of operations, destruction of data, and the theft of Personally Identifiable Information (PII) of customers can destroy the reputation of an organisation and lead to financial catastrophe
- **Compensation** – Businesses may need to pay compensation to affected parties to avoid further loss of reputation

These direct and indirect costs are not minor expenditure. The average cost of a data breach in India is [Rs. 11.9 Crore](#), which is not a cost that most businesses can shrug away. Once we combine the statistics on cyberthreats that arise due to human error or negligence with the consequences of a cyberattack, we understand the importance of managing the human risk in cybersecurity.





Real-world Consequences

Case In Point #1

Threat actors entered the IT network of Colonial Pipeline (operator of the largest fuel pipeline in the U.S.A) through a VPN account that was unused but not deactivated, by using a password that was obtained from another data breach which indicates that an employee had reused the password.

The attackers stole 100 GB of data and demanded a ransom to restore access to encrypted data. Colonial Pipeline paid the attackers [\\$4.4 million in ransom](#) (\$2.3 million was subsequently recovered) and temporarily shut the pipeline which caused a fuel supply crunch.

Case In Point #2

[Threat actors stole €50 million](#) (almost 10% of annual revenue) from Austrian aircraft part manufacturer FACC by sending an email to an employee while posing as the CEO of the company. The employee was convinced the message was genuine and transferred the funds to the attacker.

The CEO and chief of finance were not suspected of being involved in the attack, but were let go following the incident.

Case In Point #3

Target Corporation in the USA suffered a data breach that exposed the personal information of 110 million customers. Instead of attacking the company directly, threat actors used a spear phishing campaign to [compromise a refrigeration contractor](#) who had not implemented adequate cybersecurity measures. The contractor had a remote link to Target's systems for electronic billing and project management which allowed the attackers to enter Target's network. The attack caused [almost 50% drop in profits](#) for Target.



Culture as a Defence Against Error

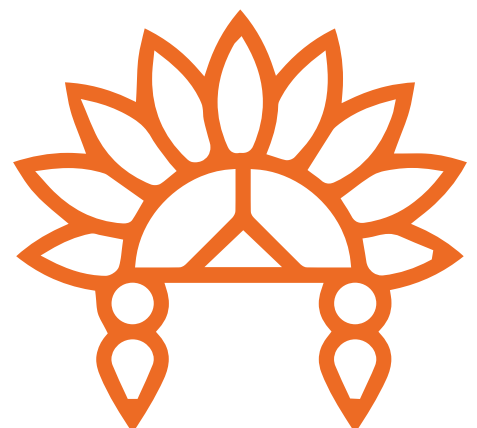
Culture is a shared set of beliefs, behaviour, and norms found in a social group and, in many ways, forms the group's identity. Every organisation has a culture which may be good or bad: a culture of teamwork that leads to customer delight is good, while a culture of sharing passwords that leads to cyberattacks is bad.

Culture evolves with or without a conscious strategy to develop organisational culture, but without a strategy it may evolve in a way that does not suit the organisation. Framing and implementing a strategy to create a cybersecurity culture will ensure that employees adopt cybersecurity as a value or way of life, and always act after considering cybersecurity implications.

What Is, and Isn't, Culture

Culture is what is practised, and not what is preached. All modern organisations exhort their teams to maintain cybersecurity, but that will not improve cybersecurity if management delays replacing legacy devices that have reached end of support and are vulnerable to attacks. Similarly, framing a cybersecurity policy is necessary, but not sufficient, to strengthen cybersecurity if the policy is not enforced.

Leaders at all levels of the organisation have to demonstrate their commitment to cybersecurity through actions, rather than words, to create a cybersafety-first culture.





Building a Culture of Cybersecurity

An organisation's cybersecurity culture is built brick by brick.



Hiring

Culture revolves around people and therefore, hiring is the first brick in building a cybersecurity culture. Hiring with an emphasis on cybersecurity should not be limited to the IT team because IT is a support function in most organisations and follows the priorities set by management. Therefore, hiring for leadership roles should emphasise the candidates' cybersecurity orientation as people follow where leaders lead. This shouldn't be considered as looking for an unusual skill as all teams are now digitally enabled and anyone with leadership aspirations should be interested in creating a safe computing environment for their team.

We have previously discussed [Case In Point #1](#) where an unused VPN account was still active, allowing attackers to compromise an organisation. Informing IT that an account is no longer in use and can be deactivated may appear to be a mundane administrative task but leaders should emphasise that such tasks need to be completed as soon as they arise, which requires leaders who understand that they are responsible for maintaining cybersecurity in their teams.

Internal and external recruitment for leaders should consider:

- The individual's awareness of cybersecurity issues, including regulatory considerations
- A track record of implementing or improving cybersecurity measures in previous roles
- How they will include cybersecurity in the plan they have for the role under consideration

Leaders, other than the Chief Information Security Officer, cannot be expected to be experts in cybersecurity but they should be known for seeking and following the advice of experts.

Prioritising cybersecurity when hiring leaders not only increases the emphasis on cybersecurity in management, it also sends a signal to the entire organisation that cyberattacks are a critical threat and countering them is now a key result area for all business functions.

Non-leadership roles also require cybersecurity skills, but the depth of skills required can vary widely based on the nature of work:

- **IT Team** – Cybersecurity is a key deliverable for IT; therefore all IT team members should have a high level of awareness about cybersecurity, and some team members will require specialised skills that are specific to your organisation's requirements e.g., you will need expertise in securing remote desktops if your organisation makes extensive use of remote computing
- **Other Teams** – Non technical teams require an attitude that puts cybersecurity first more than technical skills. A track record of conscientiousness is often a good indicator that the candidate will follow required cybersecurity measures diligently across every task, decision, and interaction



Training

We have discussed hiring with cybersecurity in mind but there are limits to the extent of weight that can be assigned to cybersecurity awareness when making a hiring decision, especially for non-leadership positions where hiring focuses on core skills. Additionally, hiring cybersecurity-oriented leaders will not cause a quick change in the organisation as awareness will take time to trickle down to all existing staff.

Training bridges the gap between the cybersecurity skills that are available and required in the workforce. Cybersecurity training programmes, such as those provided by [K7 Academy](#), can be customised to suit

- **Technical Audiences** – Exhaustive examination of organisational vulnerabilities and technical countermeasures
- **Non-technical Audiences** – Awareness programmes that can be segmented to suit the access privileges enjoyed at different hierarchy levels

Training programmes have become a critical part of organisational cyber defences because threat actors are aware that organisations deploy technology defences to protect digital workspaces; they now make use of social engineering to attack users in addition to attacks on devices or networks.

Social engineering can be fairly direct as discussed in [Case In Point #2](#) where an employee transferred funds believing the transfer request was received from the CEO. We can consider this to be a direct attack because the attacker contacted the employee at work through their work email with the express purpose of requesting a fund transfer. Social engineering, in this instance, relied on an employee being flattered that the CEO required their assistance with a special project and complying without questioning the request in their desire to gain the boss's favour.

Social engineering can be far more indirect and subtle, such as an attacker posing as a recruiter to establish contact with a member of the IT staff on LinkedIn. The fake recruiter pretends to be considering the employee for a lucrative opportunity and asks questions about the employee's current responsibilities and the IT infrastructure that they manage. The employee reveals details such as the exact brands and versions of various software in use in the organisation. The attacker can now look for known vulnerabilities in the software to attack the company. In this approach, the attacker relies on the employee's willingness to share confidential information in their desire for career progress.

Technology measures that secure devices and networks are limited in their ability to protect against attacks that target users. In the case of the direct approach discussed above, the employee voluntarily transferred the funds and no malware (which could have been spotted by a cybersecurity scan) was utilised. In the indirect approach, the employee was approached in their personal space well beyond the reach of enterprise protection.

Training and awareness programmes that focus on the various techniques used by threat actors to mislead and manipulate end-users into performing harmful actions will create an alert workforce who look out for signs of social engineering and are sceptical of messages that are unusual, unexpected, or too good to be true.

Training should also cover other relevant aspects of cybersecurity such as data privacy laws and regulations. Organisations with international clients or overseas operations will need to provide training on applicable regional laws as well.

Use of social media is an often overlooked but necessary part of cybersecurity. Training should cover appropriate use of social media for those who operate the organisation's official social media channels, and offer guidelines for sensible use of social media for all employees to follow in their personal lives. Malicious links and files can be shared through social media. Information that employees share about the organisation or about themselves can also be used to launch cyberattacks. For example, an employee may use their zodiac sign in their password which can be guessed from the date of birth they have shared on social media. Training programmes should help employees understand the risks involved in social media use.





Procurement

Procuring software or hardware usually boils down to features and price. An organisation with a culture of cybersecurity will include regular security updates as an essential feature when issuing tenders or RFPs. This involves verifying

- The vendor's track record in issuing security updates
- Duration of support, which should preferably cover the lifetime of the product

Products that are nearing end-of-support should not be shortlisted as it is risky to invest in products where the useful life extends beyond the support period. This is because vulnerabilities in the product will continue to be identified after the support periods ends but updates to protect against such vulnerabilities will not be issued by the vendor; this makes such products, and organisations that use such products, attractive targets for threat actors.

Hardware, in this context, includes networked devices like printers and IoT devices. Any device that utilises connectivity is safe to use only as long as it is actively supported.

Procurement in the cloud age should also consider where the product stores data as data sovereignty regulations should not be violated. Data security should also be verified by asking:

- i. Is the data encrypted?
- ii. How is it encrypted?
- iii. Is it encrypted only at rest or also in transit?
- iv. How are the encryption keys secured?

The cybersecurity-first approach requires ensuring, before procurement, that data is secure rather than discovering after a data breach that data is not encrypted.

Scrappage

If products that are nearing end of support should not be procured, it follows that software and hardware products that have reached end of support should be replaced even if they continue to serve the purpose for which they were acquired. Doing what needs to be done when it needs to be done is part of maintaining a culture of cybersecurity.

When scrapping devices, it is critical to ensure that any data that might be stored on the device is deleted in a way that it cannot be recovered. This requires verifying if the device stores data e.g., many multi-function printers have a hard drive that stores the documents they print, copy, or scan; this drive will need to be sanitised before the device is decommissioned or returned to the vendor.

Design

Every organisation relies on processes in addition to products. These processes should be designed with cybersecurity in mind, and anyone who designs processes should be expected to emphasise cybersecurity. This includes

- Reducing the attack surface
- Avoiding identified risks
- Having cybersecurity as a default rather than an additional layer
- Giving priority to cybersecurity issues

Cybersecurity should carryover from design to implementation and all process management activities should check if the cybersecurity component is intact. Any software designed in-house to support these processes should also be designed with cybersecurity in mind and follow the above principles.

Partnerships

All organisations have partnerships with other firms and interact digitally with their partners. [Case In Point #3](#) (mentioned earlier in this whitepaper) illustrates why any chain is only as strong as its weakest link. The firms your organisation partners with should take cybersecurity as seriously as you do, and your organisation's culture should emphasise choosing to partner with such firms.

Alternatively, your organisation can stipulate the cybersecurity standards that need to be met to qualify as your vendor with contractual penalties for non-compliance. This may be particularly important when partnering with smaller firms that may not have a cybersecurity policy or defined cybersecurity standards. Your cybersecurity culture can now become their cybersecurity culture as well.



Judging the Effectiveness of Cybersecurity Culture

We have discussed various aspects of creating a culture of cybersecurity in your organisation. The final step is judging how effective you have been at creating such a culture of cybersecurity.

You will know that you have been successful at creating a culture of cybersecurity in your organisation when teams and individuals automatically follow these measures and introduce new employees to this culture without needing to be prompted.





K7 Enterprise Cybersecurity

K7 Security combines 30 years' expertise in cybersecurity with a state-of-the-art threat research lab to deliver multi-layered, rapidly updated enterprise cybersecurity solutions that protect critical data and devices in small and large organisations around the world.

K7 Endpoint Security

The international award-winning [cybersecurity solution for desktops, laptops, and servers](#) provides enterprise-grade protection against a wide variety of cyberthreats including phishing links and websites. Other benefits include:

- **Manageability** – Complete centralised and granular control over hardware, applications, and web access
- **Cost-savings** – Lean definition updates and world-renowned low-impact protection that does not impair device performance ensure that bandwidth or hardware upgrade will not be required
- **Rapid Rollout** – Compact installers, optimised out-of-the-box configuration, and customisable endpoint installers ensure quick deployment that will not disrupt business operations

K7 Unified Threat Management

This [range of high-performance security devices](#) provide gateway security to protect your organisation's network, and include:

- **AAA Framework** – Authentication, Authorisation, and Accounting for intelligent access management
- **SPI Firewall** – The Stateful Packet Inspection Firewall with integrated Intrusion Detection System/Intrusion Prevention System (IDS/IPS) and Denial-of-Service (DoS) attack protection keeps hackers at bay
- **VPN** – SSL/IPSec Virtual Private Network for secure communication

K7 Academy

The K7 Academy offers training by cybersecurity experts backed by K7's 30-year expertise in cybersecurity. Awareness and training programmes are customised to the needs of your organisation and include:

- Fundamentals of cyber hygiene with emphasis on phishing attacks and how to spot them
- IT staff cybersecurity training to ensure that your IT team have the knowledge and skills required to secure your organisation against escalating cyberthreats





Copyright © 2021 K7 Computing Private Limited, All Rights Reserved.

This work may not be sold, transferred, adapted, abridged, copied or reproduced in whole or in part in any manner or form or any media without the express prior written consent of authorised personnel of K7 Computing Private Limited. All product names and company names and logos mentioned herein are the trademarks or registered trademarks of their respective owners.

www.k7computing.com