The Importance Of Employee Awareness In Cybersecurity For Business

A Guide to Adapting the Management Buy-in Deck for Your Company

How To Use This Deck

You might need some help in convincing your peers and seniors to commit to rolling out the Employee Cybersecurity Kit. That's why we have designed this simple, easy-to-follow presentation to help establish the importance of employee education on cybersecurity, demonstrate how Cybersecurity breaches can adversely impact your company's bottom line, and showcase the benefits of running the Kit.

These first 2 slides are a guide to advise you on how to adapt the presentation for your company's needs. Little grey "GUIDE" boxes are scattered throughout the pages to guide you on how to adapt the corresponding slide accordingly to your company.

You will need an estimated one to two hours to adapt the presentation for your company.

Objective of this deck: Offers a quick snapshot of the likelihood and consequences of a cyber attack on the business; and how an employee programme is an effective way to guard against cybersecurity threats.

What it contains:

- Statistics on how prepared businesses are in Singapore, and why employee awareness is important in the fight against cybersecurity threats
- Framework for cost-benefit analysis
- What makes a good employee education programme

Statistics for Internal Assessment

In a survey conducted by the Singapore Business Federation, senior management of companies from across industries indicated their concern that their business could be vulnerable to a cyber attack. In reality, not many invest in an holistic approach – i.e. the hardware, software and peopleware aspects of cybersecurity. The statistics offer a reality check on where your company is in awareness, understanding or actions in relation to being cyber savvy.

Incorporate qualitative (quotes, cite incidences or photo evidence) or quantitative (IT survey figures or system use numbers) information to provide as accurately as possible a snapshot of your company's situation. Get help from your HR, IT team or department heads to input data where necessary.

Cost-Benefit Analysis

To assess relative importance of business priorities, the decision to invest in an employee programme depends on the opportunity cost for a company. The framework provided in this deck guides you on what to consider for two scenarios: If no employee programme was implemented and if an employee programme was implemented.

The intention is to demonstrate how - by not implementing an employee programme - the risks and potential costs are too high to bear; and how an employee programme reduces potential costs to the company.

How To Use This Deck [continued]

Elements of a Good Employee Awareness Programme

After your senior team is aligned on the need to kick-start an employee programme, the next step is to define the extent of the first step to take. It is possible to build a rigorous employee programme by starting small and being consistent.

The slides included in the last section of this deck explain in a nutshell the habit conversion model that the Employee Cybersecurity Kit is based on, and tips that will increase the success of your employee training programme.

You'll find four types of guiding information in the little grey "GUIDE" boxes on the left side of the slides. These include:

- Reference tools and external aids to help you with the specific task
- Assistance or input that you may need from around your company
- Watch-outs
- Reminders

According to a 2016 Beazley's Survey:

GUIDE

Take a senior executive straw poll on whether they are concerned about a cyber-attack on the business. Contrast that with the company's current cybersecurity efforts.

Seek topline input from the IT department, CIO, heads of departments or HR to get a well-rounded view on the company's efforts.

While 75% said that cyber security has increased in importance for their business over the last three years, only 40% of SMEs think that their company is adequately protected against cyber security risks.

- *[Insert note on where the company is on this front]*

** Source: Beazley's Survey on the Perception of Cyber Security Risk 2016*

According to a 2015 Singapore Business Federation Survey:

GUIDE

Think about daily operational and financial constraints faced by the various functions of your company. How does the culture of your company help or hinder awareness about cybersecurity?

Seek topline input from the IT department, CIO, heads of departments or HR to get a well-rounded view on the company's priorities and challenges.

79% of businesses concerned about their vulnerability to a cyber attack cite resource, manpower, budget or workload constraints as hindering employee education.

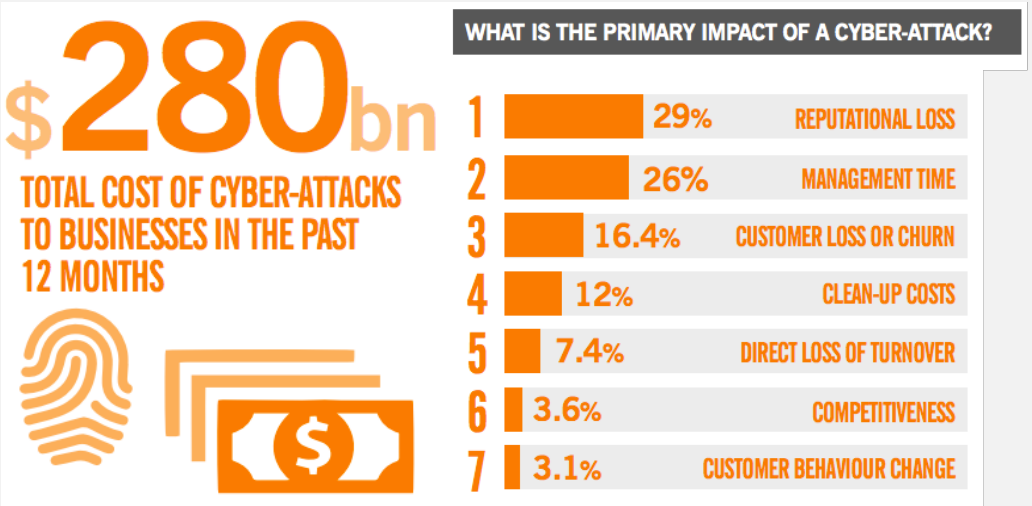
- *[Insert information on where the company is on this front]*

** Source: Cyber Security Dipstick Survey conducted by Singapore Business Federation, October 2015*

Why Is Employee Awareness So Important In The Company's Cybersecurity Efforts?

1. Data and security breaches are more common than you think

- Total costs to businesses globally have soared to **around $280 billion**, with **damage to reputation, management time and customer loss** as the primary impacts of cyber attacks.



** Source: Grant Thornton International Business Report (IBR) 2016*

2. Cyber risk is a business risk and a process of ongoing management is required

SID SINGAPORE INSTITUTE OF DIRECTORS | BOARDROOM MATTERS

Cyber security: not just for the tech-hearted

By Lyn Boxall

IN TODAY'S Information Age, where data is transmitted and consumed with the help of technology at breakneck speed, IT security threats are expanding and evolving at an unprecedented rate.

We have seen high-profile attacks on multinational companies like Target and Sony Pictures, where computer systems were disabled, business and personal data stolen and exposed to the public. In August this year, data from millions of users of Ashley Madison (an adult dating website that facilitates discreet extramarital affairs) was published as a result of a cyber attack.

Closer to home, in September 2014, hackers breached the membership database of local karaoke company K Box, threatening to expose personal information such as identification card and mobile phone numbers of more than 317,000 K Box members. Before that, in 2013, James Raj Arokiasamy performed a series of seven high-profile cyber attacks, hacking into Web servers of Fuji Xerox, *The Straits Times* blogs, the PAP Community Foundation, and the Ang Mo Kio Town Council. The Fuji Xerox attack compromised confidential data of 650 Standard Chartered clients. The affected organisations spent S$1.36 million to repair their computer systems. Raj was sentenced to five years in jail in January this year.

It is evident that cyber threats represent a real risk to Singapore companies, and the country as a whole.

The government recognises this and is ramping up cyber security measures, most notably with the establishment of a Cyber Security Agency to oversee the nation's cyber security functions. The Personal Data Protection Commission followed with the issuance of a Guide to Managing Data Breaches in May this year.

Companies need to follow suit. The International Chamber of Commerce in its cyber security guide for business (released in June) warns that "if something of value is online, it is at risk, and is likely compromised".

Cyber risk is a business risk

Unfortunately, many boards here are not adequately handling this pressing situation. Two barriers often stand in their way. The first is fear (of being overwhelmed) and intimidation (because it is a technical area that only a few are familiar with). The second is a lack of awareness and a "head in the sand" approach to cyber risk management.

Both barriers can be torn down if directors handle cyber risk in the same way as any other business risk.

That said, directors must realise and accept that cyber risk management is an ongoing process and that, while there is no assurance of ever attaining absolute security, they need to continually commit to manage cyber risk even when there is no stable end-state.

Board attention is needed

Just like any other business risk, cyber security is not an ephemeral item on the boardroom agenda, and requires three broad actions.

The first step in managing any kind of organisational risk is to undertake a risk analysis exercise. This includes prioritising the risks that justify the time and expense required to manage them. It may be trite to say that scarce financial and manpower resources mean that hard choices must be made. It is neither possible nor sensible to devote scarce resources to try and protect everything.

So an organisation must identify assets that most require protection. Management's risk analysis must enable the organisation to understand and prioritise what is important; important or critical physical and information assets are essential and therefore must be protected.

The second is leadership of the issue – starting with the board – that needs to be exhibited down the value chain. Everyone in the organisation needs to "own" cyber risk and cyber security.

Take, for example, safety in the building industry as a parallel. Once, worker safety was the responsibility of a few people – perhaps a site safety officer or a foreman. But this changed after extensive work-safety campaigns raised awareness; the point is that everyone now "owns" worker safety. Interestingly, the Workplace Safety and Health Act expressly puts the burden of ensuring a safe workplace firmly on the shoulders of the board of directors. In time, that may be the case for a cyber-secure workplace.

The third step in managing cyber risk is for the board to mandate management to have systems and processes in place to detect any security breach and to respond to it – both internally and externally – through institutionalised processes. The response must be documented, rehearsed and updated to respond to changes in the threat environment.

Being prepared

It is too late to address how to respond to a breach if it is done only after a breach has occurred. A badly executed response may do more damage to an organisation. A res- ponse showing that the organisation is in control of the situation and is reacting calmly and confidently builds trust with stakeholders.

The Cyber Security Agency of Singapore is charged with reviewing existing cyber security laws to see if they are sufficient for the evolving landscape and whether there may be a need to introduce new ones, especially when cyber crime is moving at a rapid rate. According to its CEO, David Koh, for the agency to be able to do so, it requires organisations to report system breaches in a timely fashion – something that most are reluctant to do as this may affect their reputation and possibly divulge sensitive information to their competitors. Quite pointedly, he stressed that it is a question of when, not if, a major cyber attack hits Singapore.

- The writer is a member of the Professional Development Committee of the Singapore Institute of Directors
- For more articles, go to btd.sg/BMatters

Business Times: October 5 2015

3. People, process and technology need to work hand-in-hand against cybersecurity threats

Why SMEs should step up in cyber security

By Vincent Loy

IN today's global, digital world, connectivity and data rule and everyone is somewhat connected, whether they know it or not. Safeguarding intellectual property, customer data, financial information, and ultimately your company's reputation, is a crucial part of business strategy. With the number of threats and the sophistication of attacks increasing, the issue of managing cyber risk is an especially formidable challenge for our local small and medium enterprises (SMEs).

Today, cyber risk management is clearly not a top priority for many SMEs, where their other immediate issues such as managing cash flow, increasing top-line revenue and addressing manpower shortage, etc, take precedence. SMEs typically do not invest much in state-of-the-art technology, let alone in cyber security.

It is a fallacy to think that SMEs are facing less cyber risk than larger enterprises. Many SMEs are in a state of denial that they will not be targeted for cyber attacks as they think they do not collect and store customer information in their back-end systems. On the contrary, if SMEs are not prepared for cyber attacks, they are in fact exposing themselves to a greater impact of losing their reputation and trust with their clients, and eventually even their business, when cyber incidents happen.

SMEs are a critical community in our business ecosystems. They not only support multinational corporations (MNCs) but also provide services to the governmental and private organisations which are key to national infrastructure, including electricity, transport, healthcare, etc. While some of these SMEs might not hold highly sensitive data (for example, customer data, intellectual property), they are nevertheless part of the business ecosystem and will be an attractive target for anyone trying to infiltrate into the ecosystem. Cyber criminals are discerning enough to look for points of vulnerability which provide the least resistance to their entry. As a result, SMEs are often the weak link within the business ecosystem.

Currently, many SMEs understandably choose to adopt a reactive approach in terms of cyber risk management and will only pay attention to cyber security issues when an incident happens.

The recent PwC Global State of Information Security Survey 2015 found that 43 per cent of small enterprises had experienced one or more security incidents during the past year. And that number is steadily rising. Dismally, this is only based on known incidents that were reported to the regulators and law enforcement agencies. Many others that were hit were not even reported or recorded. Perhaps they even passed unnoticed. Based on our experience, it is not atypical that a cybersecurity malware resides in the companies' systems for more than 180 days before they are discovered! With such high stakes, most would agree that information security should deserve more attention at the highest levels of an organisation.

As our digital economy continues to grow, our SMEs remain an attractive target for cyber attacks. With constrained budget, time and resources, how do we begin? Where do we start?

■ Raising cyber awareness among SMEs

It is imperative to engage management executives of SMEs to heighten the awareness and understanding of cyber threats to SMEs, the motivation behind the threats, as well as the potential ramifications and remediation options after an attack.

It is critical for the organisation to recognise that cyber risk is an enterprise-wide management issue that needs to be led from the management level, instead of treating it as a purely technology issue. Management also needs to be aware that just because they do not have customer data, they are not safe, as the reasons for cyber attack are increasingly complex and attackers are not only interested in a company per se. They might be interested in using the company as an avenue of entry or they might be interested to create havoc.

■ Understanding key risks and prioritising what needs to be done

As SMEs have limited resources, it is very critical for them to put in place at least minimal security defences such as employee cyber awareness and basic technology protection tools such as anti-virus software, followed by additional investments in the SMEs' key assets and risks. Based on the Global State of Information Security Survey 2015, 40 per cent of small businesses have estimated financial losses of more than S$70,000 as a result of security incidents.

This can be mitigated if the most valuable information and transactions are identified and given prioritised security investment. Increasingly there is a common agreement that, in the case of cyber, you only know what you know. As a result, it is important to seek an external angle and perspective of the company's internal processes and policies on a periodic basis to ensure that one is always prepared for the unknown.

■ Building cyber resilience

To ensure that SMEs are well prepared, it is important to focus on total defence which includes a robust process, enough capable people and effective technology. All too often, we see companies buying expensive cyber technology without investing in the process and people aspects. Most defences, without all three factors of people, process and technology working hand in hand, will likely remain vulnerable to cyber threats. Also, both preventive and detective measures are equally important.

Going forward, the digital world will continue to embrace smarter technologies. All businesses will continue to be even more inter-connected than ever before. SMEs will continue to be an integral part of Singapore's economy. However, the new frontier that SMEs face presents a dangerous outlook that cyber risk will continue to evolve and mutate through various interaction touch points and media.

Policies, processes and security tools that SMEs have put in place yesterday will not give them immunity against the cyber risks of tomorrow. It is imperative that SMEs continue to review and monitor their cyber security policies at regular intervals as part of their overall organisation strategy to stay ahead of the cyber battleground and build confidence for the digital future. Currently, through GoSafeOnline, the Singapore government has established broad guidelines and remediation steps against the common threat vectors.

We hope that the government, working with the industry, will continue to play a role in the SME sector to provide guidance, support and funding to assist local businesses to protect themselves and the wider community against cyber incidents.

■ The writer is the cyber risk leader at PwC Singapore

Business Times: October 6 2015

According to a 2015 Singapore Business Federation Survey:

GUIDE

When was the last time any formal or informal form of cybersecurity training was carried out in your company?

Have you come across incidences where employees displayed bad cybersecurity habits that put the company at risk?

Seek topline input from the IT department, CIO, heads of departments or HR to get a well-rounded view on how much they think employees can benefit from some sort of cybersecurity programme.

82% of concerned businesses seldom or never conduct any form of cyber security training or updates for their employees.

- *[Insert information on where the company is on this front]*

** Source: Cyber Security Dipstick Survey conducted by Singapore Business Federation, October 2015*

An Effective Training Programme Can

Positively Affect The Company’s Bottom Line

COST-BENEFIT ANALYSIS

GUIDE

This is a typical cost-benefit analysis system employed by companies determining the feasibility of investment projects.

If you or your company are used to alternative templates, just replace this section with the scenario analysis slides from your company.

In the following slides, Scenario 1 shows the net cost if no employee programme was pursued and Scenario 2 shows the net benefit if an employee programme was pursued.

For management to support an employee cybersecurity programme, the net benefit of Scenario 2 should outweigh the cost of Scenario 1.

- How much money does the company **lose** each year due to security breaches?
- What are alternative approaches to **reducing cost**?

OVERVIEW OF CURRENT APPROACH: Scenario 1

Status Quo, without Employee Awareness Programme

GUIDE

This assessment takes into consideration a mid-term (3 year) view of the investment value of an employee programme, converted into present value (PV).

Recruit Finance and Operations personnel to assist in putting value to the benefit categories indicated here.

For more tools to calculate impact of cyber breaches, visit: CyberTab

Alternatively for more references on impact monetization, refer to Resource Library of this toolkit.

COSTS	CURRENT YEAR (CY)	CY + 1	CY + 2
Investment in security hardware			
Investment in security software			
Investment in IT support			
TOTAL COST CURRENT VALUE			

BENEFITS	CURRENT YEAR (CY)	CY + 1	CY + 2
Reduction in disruption to business (e.g. prevention of security breaches)			
Reduction in loss of first mover advantage or proprietary competency			
Increase in brand equity or company corporate reputation translated as financial gain			
TOTAL BENEFIT CURRENT VALUE			

TOPLINE COST-BENEFIT ANALYSIS

TOTAL PV COSTS	
TOTAL PV BENEFITS	
NET COST (TOTAL PV COSTS – TOTAL PV BENEFITS)	

OVERVIEW OF CURRENT APPROACH: Scenario 2

With Employee Awareness Programme

GUIDE

An additional cost category of the employee programme is incorporated in this scenario.

The values of the benefit categories should increase significantly, to justify the implementation of the employee awareness programme.

For more tools to calculate impact of cyber breaches, visit: CyberTab

Alternatively for more references on impact monetization, refer to Resource Library of this toolkit.

COSTS	CURRENT YEAR (CY)	CY + 1	CY + 2
Investment in security hardware			
Investment in security software			
Investment in IT support			
Investment in employee awareness programme (Estimated staff cost or resource equivalent)			
TOTAL COST CURRENT VALUE			

BENEFITS	CURRENT YEAR (CY)	CY + 1	CY + 2
Reduction in disruption to business (e.g. prevention of security breaches)			
Reduction in loss of first mover advantage or proprietary competency			
Increase in brand equity or company corporate reputation translated as financial gain			
TOTAL BENEFIT CURRENT VALUE			

TOPLINE COST-BENEFIT ANALYSIS

TOTAL PV BENEFITS	
TOTAL PV COSTS	
NET BENEFIT (TOTAL PV BENEFITS – TOTAL PV COSTS)	

GEARING UP FOR SUCCESS:

Tips that will increase the success of your employee training programme

Success of a security awareness programme hinges on information delivery

GUIDE

Work with HR and Department Heads to identify 3 ways for cybersecurity educational messages to be integrated into existing activities or channels.

1. Security awareness training should be incorporated into new employee orientation and special training sessions by department

** Adapted from source: "Train employees - your best defense - for security awareness" Luis Navarro, Senior Consultant, Security Awareness Practice, Symantec*

Success of a security awareness programme hinges on information delivery

GUIDE

Discuss with senior management ways that performance measures can be revised to promote good cybersecurity practices.

2. Executives and managers may be more receptive to training that is incorporated into regular management meetings

** Adapted from source: "Train employees - your best defense - for security awareness" Luis Navarro, Senior Consultant, Security Awareness Practice, Symantec*

Success of a security awareness programme hinges on information delivery

GUIDE

Work with HR and Department Heads to identify 3 ways that employees can be incentivised to adopt positive cybersecurity practices.

3. A good way to reinforce what has been learned is to offer rewards and positive feedback to employees for improving their security behaviour

** Adapted from source: "Train employees - your best defense - for security awareness" Luis Navarro, Senior Consultant, Security Awareness Practice, Symantec*

Success of a security awareness programme hinges on information delivery

GUIDE

Work with the Corporate Communications team and HR to identify 3 ways to keep employees motivated on issues pertaining to cybersecurity.

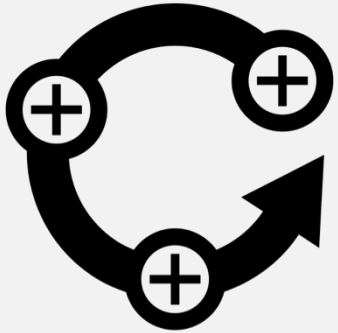
4. Announcements can be made through company newsletters or mass emails that show employees a comparison of statistics from before and after the training

** Adapted from source: "Train employees - your best defense - for security awareness" Luis Navarro, Senior Consultant, Security Awareness Practice, Symantec*

Success of a security awareness programme hinges on information delivery

GUIDE

Work with the Corporate Communications team and HR to identify 3 ways to keep employees motivated on issues pertaining to cybersecurity.



5. Seeing that others in the company are making the effort to become more security conscious will further encourage employees to continue good security behaviour

** Adapted from source: "Train employees - your best defense - for security awareness" Luis Navarro, Senior Consultant, Security Awareness Practice, Symantec*

DEPLOYING THE TOOLKIT:

How to get employees aware and then change their behaviour for the long-term

According to a 2015 Singapore Business Federation Survey:

GUIDE

It is important to emphasise the benefits of a "plug-and-play" kit, one that helps companies overcome manpower, expertise and resource issues.

For an overview of the features of the Employee Cybersecurity Kit, refer to the "ECSK Infosheet"

The **employee education digital toolkit** emerged as the most preferred cyber security enablement option for their company, ranked above structured training sessions or a combination of both.

** Source: Cyber Security Dipstick Survey conducted by Singapore Business Federation, October 2015*

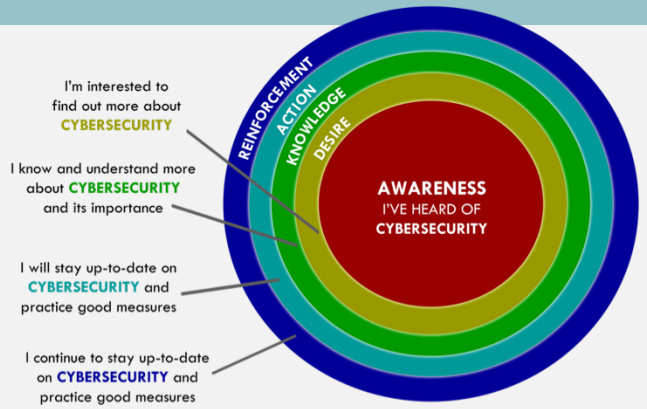
How the Employee Cybersecurity Kit has been designed

GUIDE

Explain to the senior team how the employee toolkit material is to be rolled out based on the principles of a 5-stage engagement.

Each stage of the roll-out plan corresponds to collateral or activities to be implemented.

Based on the **Transtheoretical Model (TTM) of Behavioural Change** by Prochaska and DiClimente (1983), this Employee Cybersecurity Kit helps organisations through the steps of change that will **create long-lived behaviours and assist with cultural change pertaining to cybersecurity**.

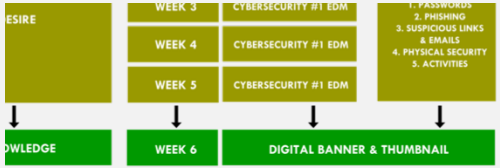


THE TRANSTHEORETICAL MODEL OF BEHAVIOURAL CHANGE
by Prochaska and Diclemente
BASIS FOR THE EMPLOYEE CYBERSECURITY KIT

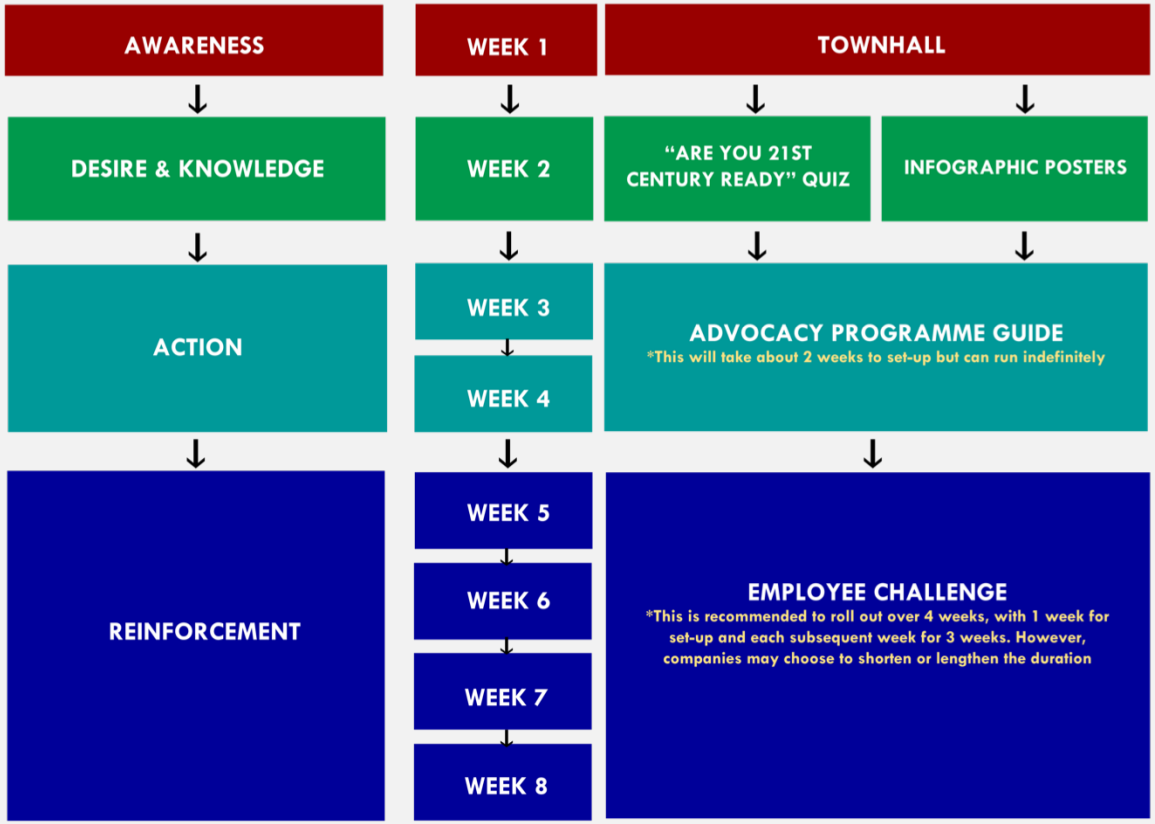
Presenting the Plug-and-Play Toolkit for your Employees' Cyber Readiness: Level 1

GUIDE

Each stage of the roll-out plan corresponds to collateral or activities to be implemented. Clicking on each box brings you directly to the collateral or implementation guide of each activity.



Presenting the Plug-and-Play Toolkit for your Employees' Cyber Readiness: Level 2

GUIDE

Each stage of the roll-out plan corresponds to collateral or activities to be implemented. Clicking on each box brings you directly to the collateral or implementation guide of each activity.