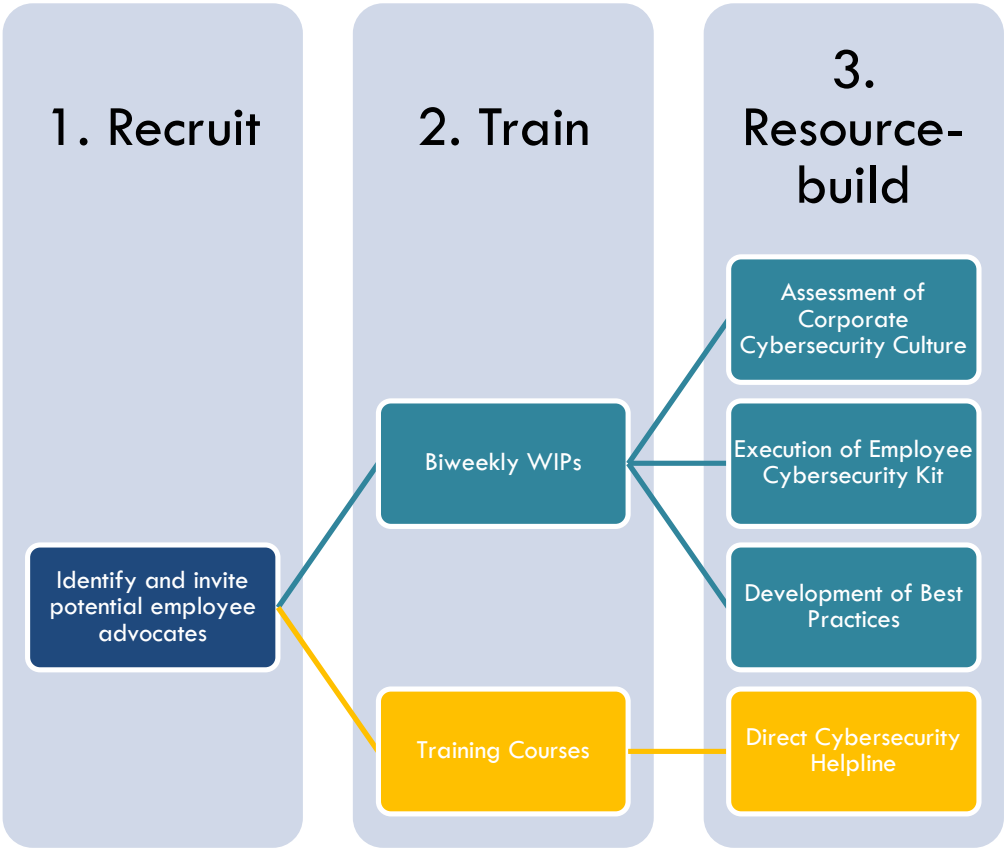
BLOCK THE HACK

EMPLOYEE CYBERSECURITY KIT

EMPLOYEE CYBERSECURITY ADVOCACY PROGRAMME GUIDE

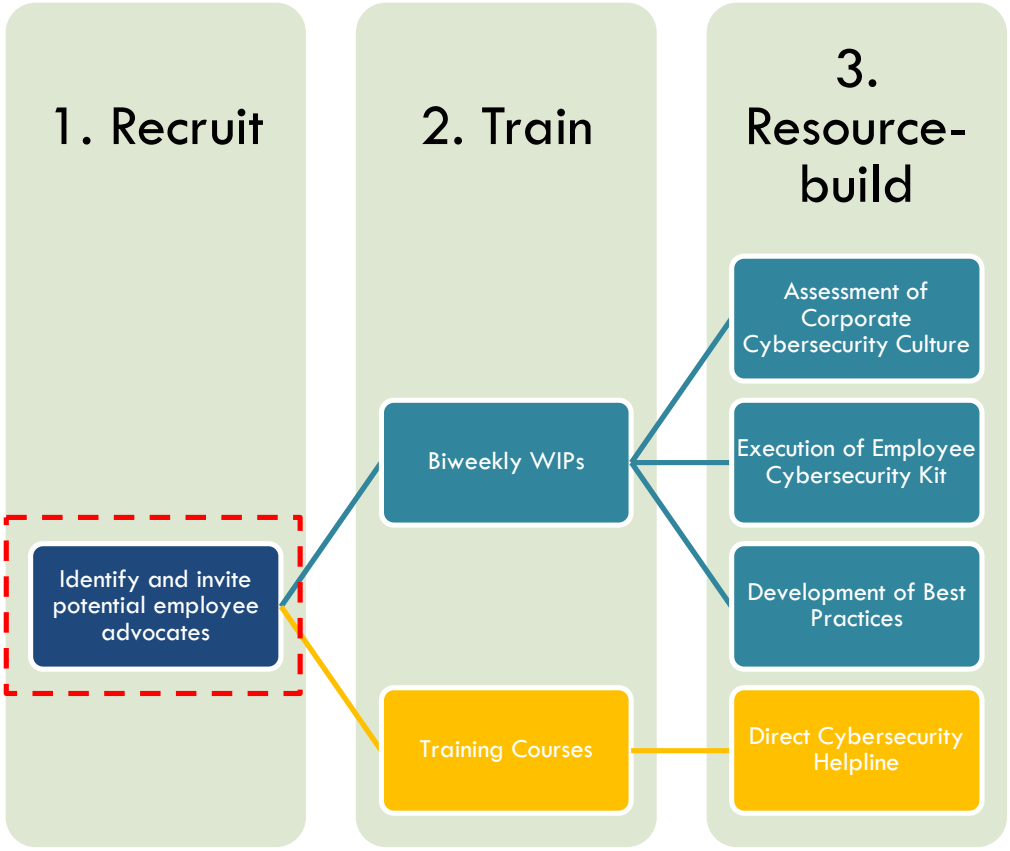
Overview



This simple, plug-and-play Employee Cybersecurity Advocacy Programme aims to build a core group of IT- and security-savvy employees and channelling their interest in technology and cybersecurity to:

- Helping the IT department field IT-security-centric questions/concerns from employees
- Helping make the topic of cybersecurity more accessible to the common employee
- Learning even more about cybersecurity through relevant courses so as to become qualified to help address basic/non-urgent cybersecurity concerns/questions
- Eventually working with the IT and HR departments to further the company's cybersecurity agenda and culture

1. Recruit



A recruitment drive of potential employee advocates will take the company approximately up to two weeks or a month, depending on how big your company is. Exact details on how to identify and recruit employee advocates can be found in the next section.

1.1. How to identify potential employee advocates

1.1.1. Criteria

- Passionate about and loyal to the company
- Have the desire to work to make things better within the company, and/or are willing to go the extra mile
- Seem to know the latest news and frequently talk about technology and cybersecurity
- Have wide circles of acquaintances and friends within the company; or are well-known for being respectful and helpful to colleagues

1.1.2. How to get started

a. Start with a few departments first, before escalating to the wider company. The departments which are more familiar with advocating for the company might include:
    - Sales
    - Marketing
    - Corporate Communications
    - Public Relations
    - Business Development
b. Speak to your department heads, and ask if they might know of any employees who fit the abovementioned criteria.
c. Search for employees on social media. Platforms such as Facebook, Twitter and LinkedIn are favoured by most employees as platforms to share views and thoughts.

1.2. How to invite identified advocates to the programme

- Your participants should have to opt into your advocacy program. It should be something they want to do.
- The easiest way to invite advocates to your pilot is by sending them a personalized invitation via e-mail. Here's a sample template that you can use:

> Hi [Name],
>
> My name is [Your Name], and I'm [Your position]. I'm launching a programme for employees who want to help make cybersecurity a more central part of our company's culture, and I was wondering if you would like to participate. I think that you would be a great fit for the programme because you already know a lot about cybersecurity and how important it is.
>
> What's in it for you? Through this programme, you will be able to:
>
> - Build your personal brand
> - Grow your professional network
> - Attain certifications in relevant training programmes and qualifications

- Develop more experience and hone your skills in cybersecurity
- And more!

I've spoken with [Name of participant's boss], and she fully supports this programme. She understands that it will only take about 2 hours of your time per week, or about 25 minutes of your time each day.

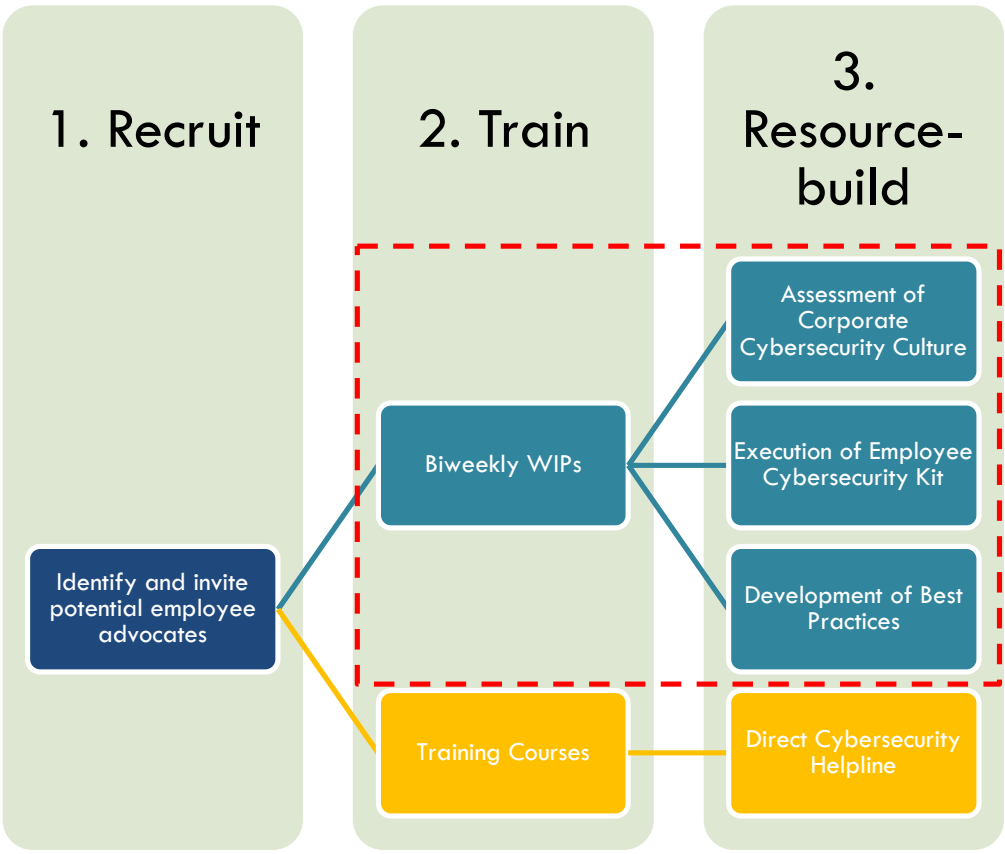
So, what do you say? Are you interested? Please let me know by [Date].

Best,

[Your Name and designation]

1.1. It is tempting to write an extremely long e-mail that explains every detail of your program. But your employees are busy. They will not read your e-mail if it gets too long. Keep it short, and focus on what's in it for your employees. Keep the details for the first meeting where all advocates get together with those of you heading the programme to discuss next steps.

2. Train And Resource-Build: Biweekly WIPs



Once you have identified and recruited your employee advocates, get them into a room and have a one-hour work-in-progress (WIP) meeting to catch up on next steps once every two weeks.

At these biweekly WIP meetings, it is important for you and the employee advocates to:

2.1. **Assess the current corporate cybersecurity culture:** This includes assessing how employees currently view cybersecurity and identifying areas which need improvement, so the team can work together to figure out how to improve these areas

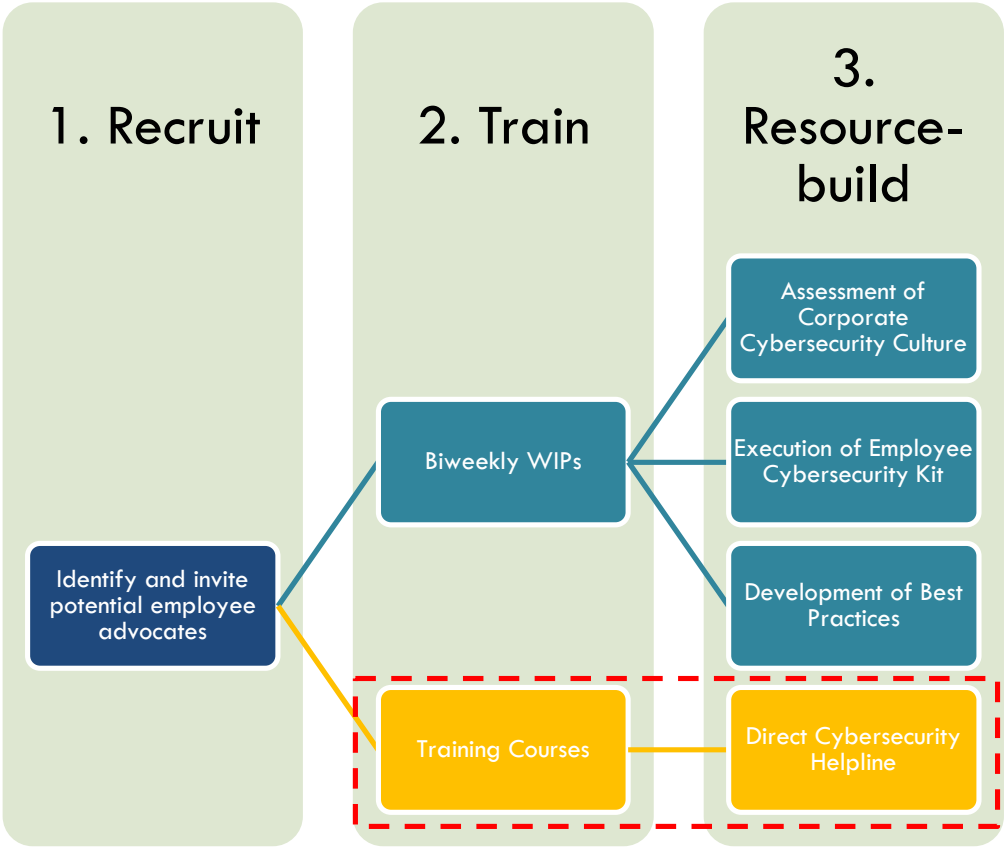
2.2. **Execute the Employee Cybersecurity Kit:** The Kit has many elements which the IT or HR department alone might not have enough resources to execute. Amongst the team, you can decide if the employee advocates are suitable for carrying out certain parts of the Kit.

2.3. **Develop best practices:** As the team starts working together to improve the corporate cybersecurity culture, certain measures will prove more successful than others.

Document these measures and evaluate why they proved more successful, in order to learn from them and apply them in future endeavours.

2.4. **Determine who is eligible for which training courses**: A list of training courses and the schemes under which the company can fund these courses can be found in your Resource Library. Each employee advocate is eligible for up to three courses for a total duration of not more than 12 days. Discuss who will be undertaking which courses at which times, so as not to strain resources.

3. Train And Resource-Build: Training Courses



3.1. How to select a training course

3.1.1. Criteria

- Level of qualification of your employee
- Scope of the curriculum and its relevance to your company
- Availability of external funding

3.1.2. Available Training Courses

Companies are encouraged to refer to your Resource Library here for the latest list of cybersecurity training courses and funding schemes available.

For a cursory overview, the table below compiles the main recommended courses (at the time of publication) for your employees and indicates whether or not they can be funded by either the SkillsFuture scheme or the Productivity and Innovation Credit scheme (PIC).

Title/URL	Description	Eligible for SkillsFuture/PIC funding?
Entry-Level Courses		
IT Risk, Governance and Security	Offered by Singapore Management University, this course offers a good understanding of the various risks, threats and vulnerabilities that confront organisations today and the mitigation actions and governance disciplines that need to be incorporated to control and contain possible IT risks and security concerns.	Yes
Systems Security Certified Practitioner (SSCP)	Offered by DigiSAFE Cyber Security Centre, the course offers SSCP CBK curriculum integrated with hands-on training. It also provides a comprehensive review of information security concepts and industry best practices.	No
Securing Enterprise IT Systems and Infrastructure	Offered by Temasek Polytechnic, this course provides an overview of security concepts and issues relating to the IT systems and infrastructure of an enterprise. It will cover IT Security operations and best practices, with a focus on minimising IT security risks in an organisation.	Yes
Intermediate Courses		
Specialist Diploma in Information Security	Offered by Nanyang Polytechnic and Singapore Institute of Technology, this course is designed for IT professionals to improve their capabilities in architecting, designing, developing and managing effective IT security solutions.	Yes
Certified Security Analyst	Offered under the National Infocomm Competency Framework, this course provides foundational knowledge of security topics and managing security systems and incidents.	Yes
Cybersecurity Operations Specialist	Offered under the National Infocomm Competency Framework, this course focuses on the cognitive and analytical abilities of participants, in addition to knowledge. NICF CSOS' emphasis is on equipping participants with cyber defence operational skillsets – that will be ingrained in individuals on a day-to-day basis.	Yes
Diploma in Security Management	Offered by Temasek Polytechnic, this course is developed to equip officers with managerial skills and competencies to perform the job at managerial level and manage the security operations, agency or	Yes

	department.	
Certificate in Security Operations	Offered by Temasek Polytechnic, this course equips the security officer with basic and specialised skills to enhance the officer's work performance.	Yes
Advanced Courses		
Cybersecurity Incident Response and Management	Offered by Temasek Polytechnic, this course provides an introduction to the processes behind cybersecurity incident response and management, with a focus on assessing the impact of incidents on businesses. It will also include how to implement effective methods of collection, analysis and reporting in an SOC (Security Operations Centre).	Yes

3.2. How to set up a direct cybersecurity helpline

Once your employee advocates are adequately trained, they will be able to help the IT department in fielding and addressing IT-security-centric questions and concerns from other employees by setting up and crowdsourcing a direct cybersecurity helpline. This can be done through a couple of ways, depending on what is convenient for a company your size:

1. Instant messaging chat group on a mobile app (e.g. WeChat, Whatsapp etc.)
2. E-mail group (e.g. cybersecurityhelpline@yourcompany.com)
3. Intranet group
4. Social media account (e.g. Facebook, Twitter etc.)

This direct helpline will allow employees to feel that their cybersecurity concerns can be readily addressed thereby decreasing their sense of helplessness when it comes to a seemingly complex issue such as cybersecurity.

4. Programme Benefits For Advocates And Company

4.1. Advocates

- **Company-wide recognition** - Sometimes, acknowledging excellent service is enough for your employees. You can give your advocates a special thanks in a company-wide meeting. If you want to throw in an added benefit, you can award them small trophies or plaques.
- **An ongoing rewards programme** - For every quarter a person participates, she receives a reward. It could be a t-shirt, a gift card, the latest headphones, etc.
- **Support from department heads and management** – Employee advocates will need to put aside 25 minutes of their time each day to devote to carrying out this programme. Department heads and management will need to be able to support them in putting aside time which could otherwise be used for work to participate in this programme.
- **Official certification/qualification in cybersecurity** – Aside from support to carry out the programme, the company should also support the employees in pursuing official certification or qualification in cyber-security-related fields. Each employee advocate is entitled up to three programmes that will take no longer than 12 working days in total to complete. A complete list of courses that employee advocates are eligible to sign up for can be found in the Resource Library HERE. Companies are encouraged to utilise the Productivity and Innovation Credit Scheme, and the SkillsFuture scheme, to fund these courses.

4.2. Company

- **Increased awareness and understanding of cybersecurity amongst employees** – With employee advocates to make cybersecurity seem more accessible to other employees, and ensuring that there are ample qualified employees to help increase the cybersecurity of the company, the company can slowly start to integrate cybersecurity as part of the corporate culture. This will eventually help protect your company better against cyber threats.
- **Increased support for your company by your employees** – Employees today are looking for more than just a 9-to-5 job. They want to be involved in their work, enthusiastic about the organization they work for, and committed to their fellow workers. Employee engagement has long been identified as a way to make them feel more involved in and committed to the company.

- **More efficient use of current resources** – Rather than employing new resources or over-taxing already taxed resources (such as the IT department), recruiting employees outside of the IT department to help share the cybersecurity agenda will be more efficient. The employee advocate programme is a way to crowdsource knowledge, understanding and assistance in cybersecurity.
- **Possible model for future employee advocacy programmes** – With this template for creating your own Employee Cybersecurity Advocate Programme, you are now equipped to create other types of employee advocate programmes to further your company's agenda and tap on your employees to speak up on your behalf.

Tips to Get Started

- Keep it small first. Start out with 3-5 employees, depending on the size of your organisation first, and develop a base of best practices with them first.
- If necessary, identify the key roles that you wish your employee advocates to take. This guide here gives a good overview of the kinds of roles you may wish to encourage within the programme, so as to ensure that everybody involved feels like they have a choice as to their level of participation.