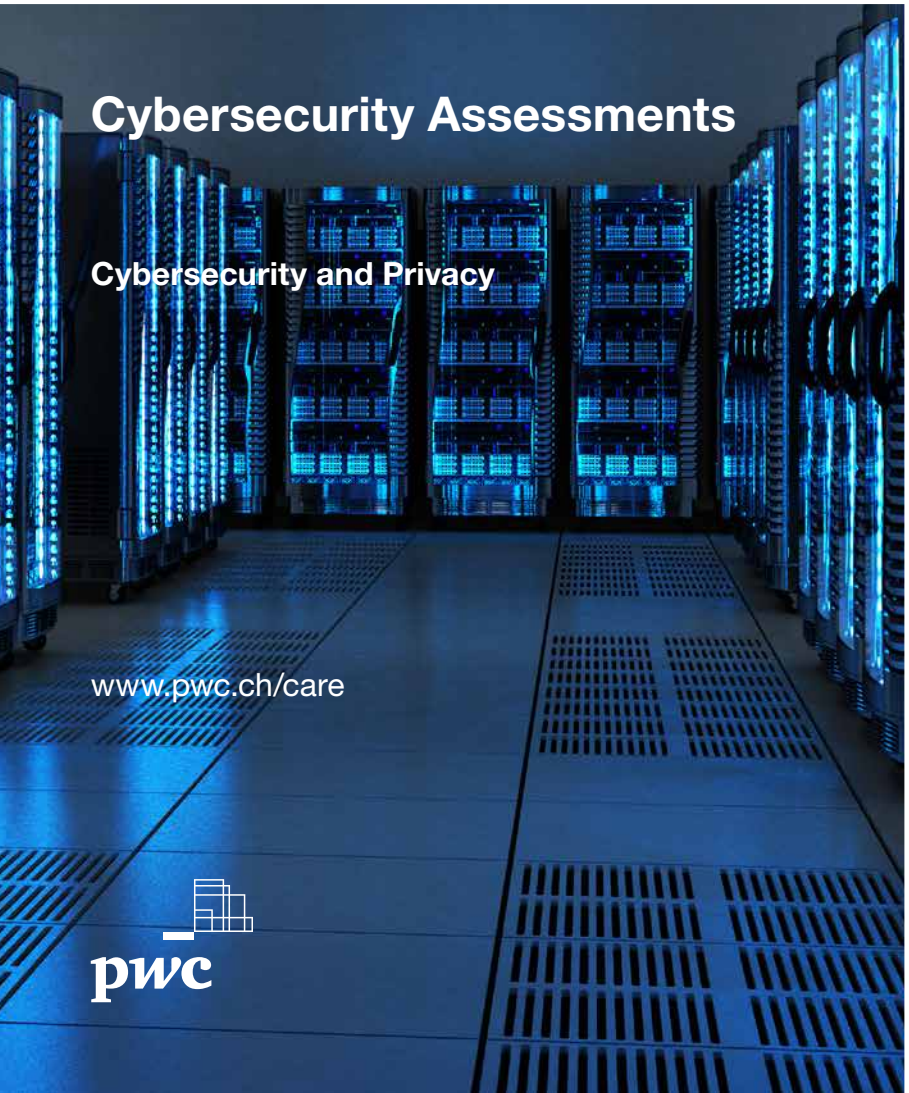
Cyber Attack and Readiness Evaluation



Cybersecurity Assessments

Cybersecurity and Privacy

www.pwc.ch/care

pwc

Cybersecurity at PwC: we focus on risks

Cyber Attack & Readiness Evaluation

CARE is a new service designed by PwC to help clients evaluate their security posture – their ability to deal with the main threats of our cyber world – in an easy and understandable way.

How does CARE work? First, we do a workshop with you to evaluate online your risk appetite and the measures currently in place to mitigate your exposure to the main cyber risks. We then challenge these responses with a technical evaluation of your readiness.

This service is primarily designed for small and medium-sized enterprises, but it is modular and scalable to any size and field of activity. We have credentials in a range of industries including public administrations, banks, consumer and luxury goods.

Our modular approach includes five services covering the three dimensions of cybersecurity:

Processes are the back-bone of any organisation.

Our Service:
- Cyber Risk Evaluation

Cybersecurity is deeply involved in technology.

Our Services:
- Vulnerability Scanning
- Penetration Testing

Often presented as the bottleneck in cyber security…

… people, if trained correctly, can be a central resilience component.

Our Services:
- Phishing Awareness Campaign
- Cyber Awareness Workshop for Executives

Cyber Risk Evaluation

Service overview

Know the risks before it starts to hurt

The purpose of a Cyber Risk evaluation is to identify potential problems before they occur. This enables you to plan risk-mitigating measures and invoke them as needed across your information systems or projects.

In this phase, we will go through an online questionnaire to evaluate your risks and the maturity of your security controls. We have based our set of controls on the ICT Minimum Standard from the Switzerland's National Economic Supply (NES) organisation.

Deliverable

Pragmatic recommendations

- A report with a complete list of severe cyber risks and an executive summary summing up your current maturity level
- For the defined scope, a detailed report in an electronic format that will be prepared for and presented to various bodies within your organisation
- A project plan covering all project activities planned at all phases of the engagement after the initial mobilisation phase

Vulnerability Scanning

Service overview

What are the open windows?

An external vulnerability scan is a simple out-of-the-box solution for rapidly identifying weak points in your company's network that could be exploited by hackers.

Deliverable

Gives your IT Department clear tasks and a roadmap

You will receive an exhaustive report with a list of the known vulnerabilities discovered while performing the scan. The report will also outline the steps needed to fix these vulnerabilities (i.e. the relevant patches to apply).

Penetration Testing

Service overview

Get in!

Whereas vulnerability scanning assesses but does not exploit vulnerabilities, penetration testing seeks to prove the existence of a vulnerability by actually exploiting it. Penetration testing discovers the depth of the problem and finds out exactly what type of damage could be done if a vulnerability were exploited.

Deliverable

Observations and recommendations

We deliver a pragmatic report listing observations and recommendations, including quick wins. It describes the methodology used for our penetration exercise, the assumptions taken and the business impact of the 'hack'.

Phishing Awareness Campaign

Service overview

Challenging the 'weakest link'

Phishing is the most frequently used technique by hackers to gain an initial foothold in a company's network. Phishing enjoys a high success rate as it targets the weakest component of the security chain: human beings! Our awareness campaign simulates a phishing attack by sending a credible email to a defined group of people asking them to perform a particular action (for example clicking on a link or opening an attachment) which could compromise the end-user device or lure the recipient into disclosing confidential information.

Deliverable

A report on how to be 'phished' less

Every action of the tested group will be recorded and summarised in a report. It will outline the response of your employees (e.g. the number of people who clicked the link, opened the attachment and provided their credentials) so that you can effectively gauge their level of awareness and/or determine the effect of any training they may have done in this area.

Cyber Awareness Workshop for Executives

Service overview

Awareness training for executives

Given the rapidly evolving nature of cyber risk, company directors and executives have to be kept regularly up to speed on the salient technology and developments in cyber risk.

Our Game of Threats™ session will help your executives or colleagues understand, try out, iterate and play a near real hack use case with our interactive tool.

Deliverable

Awareness report

You'll receive a presentation which summarises the key findings observed during our session with practical actions.

Our modular approach

We have designed a scalable and adaptive service model to gear our services to your needs and size. Depending on the depth of the assessment required and your experience and knowledge of cybersecurity, you may need a certain level of technical and human behaviour evaluation. Let's tailor your package together!

	Process	Technology	People
Basic	Cyber Risk Evaluation > Online self-assessment > Workshop with our cybersecurity experts	Web Application security assessment (Blackbox) > Assessment of a small dedicated website/ e-commerce application	Phishing exercise «Click & Download» > Up to 50 employees
Advanced	Cyber Risk Evaluation > Online self-assessment > Several workshops with our cyber-security experts, including workshops with your IT/Security providers	Web Application security assessment (Grey box) > Assessment of a medium sized application such as an e-banking/ payment processing system or medium sized CRM/ERP	Phishing exercise «Click & Download» > Up to 100 employees
Extended	Cyber Risk Evaluation > Online self-assessment > Workshop with our cybersecurity experts > Control testing based on the NIST Cybersecurity Framework	Web Application security assessment (White box) > Large website with complex CRM systems or web applications based on SAP/Oracle/Microsoft	Phishing exercise «Click & Download» > Up to 250 employees Cyber awareness workshop for Executives > Game of Threats™

Contacts

Please contact us to get an initial evaluation of your needs and find out how we can help you evaluate your risk and support you to get better prepared.

Yan Borboën
Partner
Cybersecurity and Privacy
+41 58 792 84 59
yan.borboen@ch.pwc.com

Urs Küderli
Partner
Cybersecurity and Privacy
+41 58 792 42 21
urs.kuederli@ch.pwc.com

Alexandre Baranov
Manager
Cybersecurity and Privacy
+41 58 792 92 76
alexandre.baranov@ch.pwc.com