cykur
Let's Be Cyber Secure

www.cykur.com

A Cybersecurity Primer Education for Small Business Managers

Small and **Midsized Businesses (SMBs) are the target of 80% of cyber-attacks** perpetrated in the USA. **60% of the victim companies fold within six months** of an attack because it takes them **21 days to recover**. Benjamin Franklin summed it up perfectly:

"If you fail to plan, you are planning to fail"

We are offering four one-hour sessions during which you will learn **how the criminals are organized** and the levers they use to fool their preys and **how you can outsmart them**.

There are no too small companies or individuals for bad actors to extort some money or stall your business to a halt.

The program

We all have **limited resources** whether it is time or money. As a result, **we push back** on addressing the risk that feels remote and indeed **virtual, until they hit!** We have put in place an **affordable and manageable training solution that is accessible to leaders with no IT background, with an** aim to help organize your company in **mitigating cyber risks and guiding small companies to Prepare, Respond, and Recover.**

The program consists of four one-hour live sessions **led by a renowned expert via Zoom** over a one-month **period**.

Pricing: $575*

Contact US
For Availability

Agenda:

First Week:
Cyber security landscape and best practices. A very lively training, during which you'll get to discover the organization of cyber criminals to better counter their approach, as well as, policies and procedures to protect everyone in the company and help them be aware of the threats.

Week Two:
The enterprise cyber risks landscape. We will go deeper in understanding how the bad actors get to observe your company once inside your firewalls and how they plan their attack accordingly. We'll offer best practices to limit their ability to maneuver.

Week Three:
Mapping your “crown jewels”, organizing your data and segregating access rights. We propose a framework to build your own Cyber Incident Response Plan, as well as, the policies and procedures to structure your company’s cyber posture.

Week Four:
Testing your Cyber Incident Response Plan. Recovery steps in case of a breach. When the house is on fire you have little time and you don’t think straight, your reptilian brain takes over. Rehearsing is key to maintain a sound response. You also need to be clear as to how you will get back on the saddle and communicate with your vendors, clients, employees, …

Bonuses:

You will receive a link (valid only during the time of the training) giving you access to material templates presented during the course, as well as, a library of valuable documents compiled by the presenter.

Presenter:

Philippe Flichy
Founder and Principal of Cykur

Philippe is a seasoned fortune 500 executive who contributed (among many other assignments) to the security of the 2002 Salt Lake Olympics intranet and has demonstrated a strong entrepreneurial spirit during his very successful career.
Philippe Flichy has created several companies and has been an executive for Fortune 500 companies. He is a long-time member of Infragard (a partnership between the FBI and members of the private sector for the protection of U.S. Critical Infrastructure). This puts him in a unique position to best figure out how to help SMBs build their cyber resilience. Philippe graduated from Boston University in Management Information Systems and is a Certified Cyber Security Architect

A proud member of

www.cykur.com phil@cykur.com https://www.linkedin.com/in/flichy/

Cyber security protection myths (random picks):

My data is safer in the cloud
Roughly half of all corporate data is stored in the cloud, and companies might be putting too much trust in how it is secured. "Surely that data is as precious to cloud service providers as it is to the companies who produce and rely on it, right? Wrong," says Simon Jelley, general manager for SaaS protection, endpoint and backup executive at Veritas Technologies.
Many cloud providers don't provide guarantees that a customer using their service will have their data protected. "In fact, many go as far as to have shared-responsibility models in their terms and conditions, which make it clear that a customer's data is their responsibility to protect," Jelley says.

We are too small to be a target
Even today, too many companies believe they are not relevant enough to fall victim to a cyberattack. "If you have an exposure, you are a target…and everyone has exposure," says Bramson. "Cyber attackers can specifically target a company, or they can set out general attacks, to see who gets caught in their net. Either way, you will suffer an attack at some point." Customer data is a valuable commodity sold on the dark web, and compromised websites can deliver malware. "SMBs often lack the resources to implement and manage a proper information security program making them easy prey," says Giaquinto.

Cybersecurity is an IT responsibility
But the thing is, **cybersecurity is everyone's problem and responsibility**. In a functioning business, your company is only as strong as your weakest link. 95% of breaches involve some form of human error.

Sponsored by:

SEAMLESS SOLUTIONS

* For the full four sessions and the templates. Group size: five participants minimum.

Cykur helps SMBs **build a strong cyber posture** by adapting standards used by large companies to an affordable and manageable level for small to mid-size businesses. We guide companies to **Prepare, Respond,** and **Recover**.

Cykur help business owners and CEOs that have grown to the point that they need to implement or adapt **IT security protocols** and **be more strategic** with **how they protect their systems and data**.

Contact us on in	Follow us on	Visit our Web Site