



Defenders of our cybersociety

Start Winning Your Cyber Security Battles Today!

Do you want to STOP SPENDING Security budgets INTO what looks like A BLACK HOLE?

Do you wonder how to START WINNING against hackers that are global, well-funded and professionally organised?

Are you looking for a cyber, IT or information security strategy that will SAVE MONEY and is effective at the same time?

Do you wonder: WHAT SHOULD I DO FIRST with my limited resources to best protect my organisation?

ACT NOW: Follow the leading adopters that have shifted from a compliance only focus to a REAL and AUTOMATED security focus?

The cyber security reality your organisation is facing...

There are 2 types of organisations: Those that know they have been breached and those that don't.

Which one are you? Are you blind like most organisations?

69%

of breaches are first spotted by external parties, 9% by customers.



66%

of breaches remain undetected for months or even years.

In today's cyber world every organisation is targeted. Saying that your organisation will not be hacked is as naïve as stating that you will never be sick or in need of a doctor. What you want is to timely detect an illness before serious damage occurs. Several recent independent reports confirm that most organisations are failing to detect cyber breaches themselves. And what is most worrying is that most breaches get a lot of time to further spread undetected once inside the organisation, leading to the bigger damages and losses.

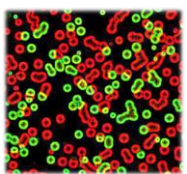
What you should really be worried about...

1. Are you sure you can early detected malicious activities once they get in?



It is a reality hackers will break in, that is why you want to focus, or shift, a significant amount of your efforts towards detection instead of preventive measures that are typically in place like firewalls and anti-virus.

2. Will you know which systems and information has been compromised?



Once you detect a breach, your first questions will be: Which systems do I need to clean? What data might be stolen or copied? If you can't answer these questions you might have to publicly disclose more than you want and/or pay a higher legal fine than would strictly be needed. Additionally you will be looking for many very expensive needles in your haystack while trying to clean your systems.

3. Do you have an incident response capability that can act on incidents?



When a breach is detected you need to respond as soon as possible to prevent further damage. You will need the correct amount of resources and processes in place for your organisation.

4. Do you have a communication plan?

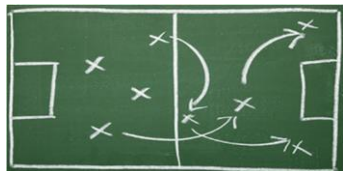


If you value your reputation, establish action plans and processes to respond to the media, and other stakeholders. You better prepare this sooner than later.

Where do we start, and how can we afford this?

In order to make any cyber, IT or information security strategy affordable and effective, organisations should use the following guiding principles as key drivers in selecting security controls.

Principle 1: OFFENSE drives the DEFENSE



First, put controls in place that block the most common attacks used today. Make sure that you understand how attacks typically enter and spread into organisations and clearly prioritize your efforts based on this. Many good reports based on real forensic investigations are available today.



Principle 2: Prevention is ideal, but DETECTION is A MUST

Typical preventive controls like firewall and anti-virus are too easily bypassed, other controls are too expensive or are not acceptable for your users. A realistic cyber security strategy focusses at least 50% of efforts on detection.



Principle 3: Automate, automate, AUTOMATE !

Hackers automate, if you don't, you are either lost or spending too much money. Any control that you select must be automatable.

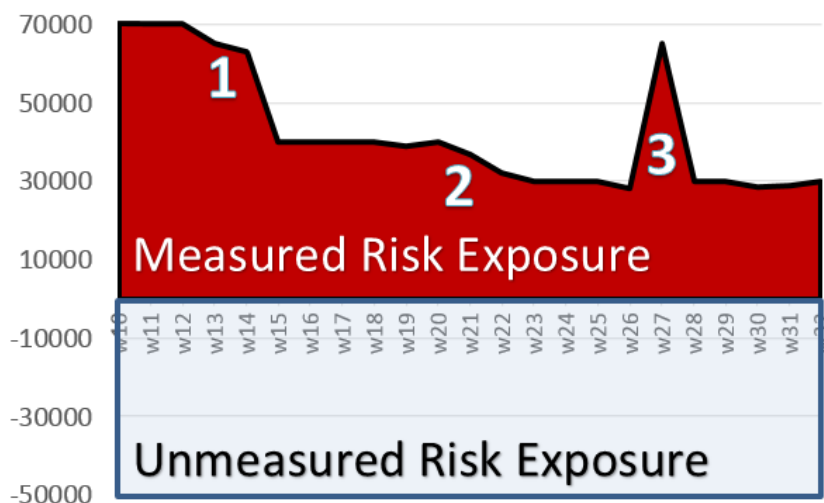


Principle 4: Transparent and measurable REAL-TIME security METRICS

Define a set of security metrics that you can fully automate and gather in real-time. Publish them throughout the organisation for managers to understand, IT to implement and auditors to verify. Share a common goal.

Case in point: Avoid decisions based on emotions and end-less debates about what is 'safe'.

Step by step make the most important risk exposures visible. Have validation scanners continuously scan you infrastructure to measure the risk and compliance with your security baselines. Implement tools and enforce more security controls that further reduce your risk exposure.



Event 1: A continuous patching policy is approved and automated patching technologies implemented.

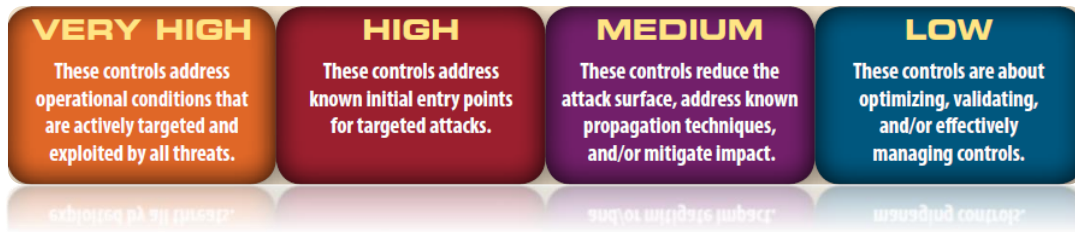
Event 2: A decision is enforced to turn on personal firewalls on workstations and laptops.

Event 3: A human error resulted in 50% of all deployed anti-virus software to be disabled. The issues was detected in the risk score and quickly remediated.

Find your FIRST answers in the SANS 20 Critical Security Controls

The 20 Critical Controls is the only framework that fully follows the guiding principles explained. They don't only tell you WHAT to do, but also HOW it can best be implemented and what you should do first.

The controls are prioritized in 4 categories:



They have been put together by the best international experts and cyber security fighters in the world. Leading adopters include the U.S. National Security Agency, the British Centre for the Protection of National Infrastructure, and the U.S. Department of Homeland Security.

If you want to know more about the SANS 20 Critical Security Controls and our approach to set these up in your organisation, contact us for a free presentation.

About Krinos

We defend our cybersociety against the growing number of cyber threats in order to allow our society to prosper and evolve more safely into the digital age. We seek to protect 4 key pillars of our society: critical industrial infrastructures, medical systems, our intellectual property, and financial systems.

Krinos is specialised in IT & information security consultancy and positions itself as an independent partner. Our employees possess a unique mix of technical hands-on engineering and consulting skills. We invest time and resources to learn about existing open-source and commercial technologies in order to give better advice. We are no-nonsense, practical and to the point.

We advise and guide organisations with the strategy, definition and technical implementation of security projects. We take ownership in aligning the existing business, operational and technical context.

If you would like more information on Krinos services or want to contact us:

www.krinos.be/cybersecurity
Loveld 9, 3212 Pellenberg, Belgium
cybersecurity@krinos.be
+32 499 99 85 07

