10 leading practices to combat cyber threats

1. Board support
   Organizations need executive support to establish a clear charter for the information security function and a long-term strategy for its growth and funding.

2. Governance
   Management must have in place a robust information technology risk management framework from which the organization's cybersecurity policies, procedures and operating model can be created and sustained.

3. People
   Today's information security function requires a broad range of capabilities with a diversity of experiences. Technical IT skills alone are no longer enough. Security functions also require a clear articulation of roles, responsibilities, and reporting lines.

4. Technology
   Information security functions must supplement their technology deployment efforts and knowledge with strategic initiatives and expenditures such that technology support the operational risk appetite of the organization.

5. Awareness
   Firms need to provide security awareness training to its personnel to increase awareness of cybersecurity risks and good security hygiene.

6. Asset inventory
   Organizations must establish and maintain an inventory of their electronic and physical assets (i.e. mobile device, laptops, infrastructure hardware) and who has what access to them.

7. Vendor risk management
   Organizations need to understand the security measures at their vendors - who has access to their data at each point within the transaction life cycle from inception to recording and that data is secured in transit, in use, and at rest.

8. Reporting
   Information security requires an environment that includes a well-maintained enterprise event monitoring and incident/problem management tracking system to track and manage events associated with business priorities and assess the true risk and impact to the organization.

9. Continuous monitoring
   Signature and rule-based tools are no longer as effective in today's environment. Instead, information security functions may wish to consider using behavior-based analytics against environmental baselines and have incident response plans in place.

10. Continuous improvement
    Organizations must establish a framework for continuously monitoring performance and improving their information security programs in the areas of people, process and technology as well as re-evaluating the accepted levels of risk.

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2015 Ernst & Young Cyprus Ltd.
All rights reserved.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.
What you haven’t seen can really hurt you
Cyber attacks, data loss, application vulnerabilities, external and internal access to sensitive and confidential information, and the increased use of third party service providers – all pose a threat to your existing technology infrastructure and your operational business processes.

As the threat landscape rapidly changes and risks increase, companies need to change their mind set and approach toward information security and privacy to address a new normal. They need to operate under the assumption that unauthorized users are accessing the company’s information technology (IT) environment on a daily basis - to assume “they’re in.” Cyber breaches can impact shareholder value, tarnish the brand and expose the company to litigation. These are issues of importance to the C-suite, elevating the need for boards of directors, audit committees, general counsels and chief risk officers to work alongside information security and privacy officers. This collaboration needs to fully address their organizations’ risk management level of due care, approach and preparedness.

EY’s Information Security practice offers a wide range of management, assessment and improvement services, ranging from cybersecurity diagnostics to our security program management assessments and our cyber threat/vulnerability assessments. These services help our clients maintain the appropriate alignment between their security, IT and business strategies, enabling them to maintain their focus on their business needs while addressing their security and risk issues.

Several recent high-profile, front-page headline cyber attacks are serving as a wake-up call for the C-suite. In fact, executive and board-level awareness of cyber risk appears to be at an all-time high – and growing.

Cybersecurity diagnostic
A cybersecurity diagnostic will provide your organization with an overview of your current cybersecurity posture within the context of your firm’s overall business objectives and provide a summary roadmap and recommendations to strengthen your cybersecurity program.

What can EY do for you?

- Provide a current-state analysis of your information security program
- Assess security capabilities across the EMEA cybersecurity examination domains
- Provide recommendations and next steps to help you enhance your overall cybersecurity program including, recommendations for additional measures to reduce your cyber risks and support addressing regulatory requirements

62% of organizations have not aligned their information security strategy to their risk appetite or tolerance
EY’s Global Information Security Survey 2013

What sets EY apart:

- Objective results – We provide clear and pragmatic guidance to your organization. EY’s proven approach and trained professionals deliver reports and recommendations that are right-sized for your organization and easily understood by senior executives, including the board of directors and risk and audit committees.
- Industry leader – As a leading professional services organization, EY’s brand reputation lends weight and credibility. We provide a broader, business-based risk focus coupled with a technology lens and solid brand confidence supported by approximately 2,000 asset management professionals.
- Advanced security centers – We offer sophisticated technical facilities and dedicated security professionals who assist our clients 24 hours a day, 7 days a week. Our globally integrated laboratory centers are based in strategic locations throughout the Americas, EMEA and Asia-Pacific and have performed hundreds of war games and red-team attack and penetration exercises.
- Unique methodology – EY provides services to help you develop policy and process recommendations and control recommendations, and we assist with the co-development, design and implementation of selected information security and information protection measures to meet regulatory requirements.

Customized cybersecurity services
EY’s customized cybersecurity services are tailored specifically to your organization and its needs. These services offerings include cyber threat and vulnerability assessments, security program management assessments, IT risk management, IT risk assessments and cybersecurity training/awareness.