Are you safe?

Your business growth strategies are at the heart of the cyber risks your organization faces

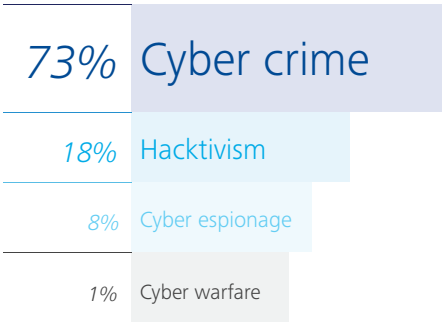
Most reports on cyber security revolve around a common theme: despite heightened attention the number of cyber incidents–and their associated costs–continues to rise. They typically point to the growing sophistication of hackers and other adversaries as a particularly intractable problem, and some deliberate over whether being secure is even possible in today's rapidly evolving landscape of cyber attacks.

Global cyber crime statistics and costs of cyber crime paint an equally alarming picture:

≈ 1.6M

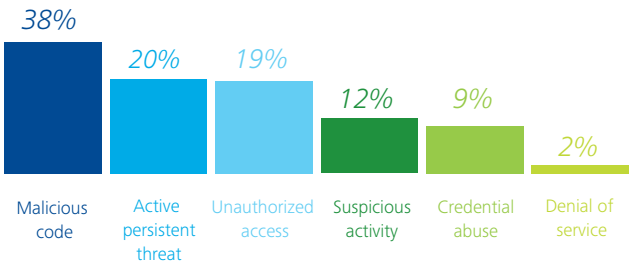
New cyber threats are being identified everyday globally

The major motivation behind cyber attacks



Top 5 industries attacked in 2014

Categories of incidents in 2014



*Statistics provided by Symantec's Internet Security Report 2013 & Ponemon Institute - The Impact of Cybercrime on Business Report 2013

The cost of cyber crime

Estimated annual cyber crime cost to consumers

≈ US$144B

Estimated annual total cost of cyber crime

≈ US$444B

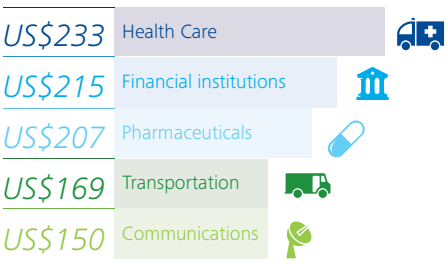
Estimated number of adults that fell victim to cyber crime

≈ 431M

2014 largest single cyber crime cost

≈ US$189M

Top 5 per record costs by industry



2013 average per capita cost per data breach

≈ US$194

2013 average number of breached records per incidents

≈ 28,765

2013 average total cost (indirect/direct) of data breach

≈ US$5.4M

* Statistics provided by Symantec's Internet Security Report 2013 & Ponemon Institute - The Impact of Cybercrime on Business Report 2013

The Middle East in particular is on high-alert with three dimensions of threat elevating the level of risk above global averages:

Regional geo-political instability

The growing political instability in various conflict zones throughout the Middle East has given rise to numerous hacktivist groups that have wreaked havoc on public and private institutions, both regionally and globally. These notorious, self-professed electronic armies use malicious and destructive techniques to undermine the security of the Internet as a means to promote political ends.

Perceived economic wealth

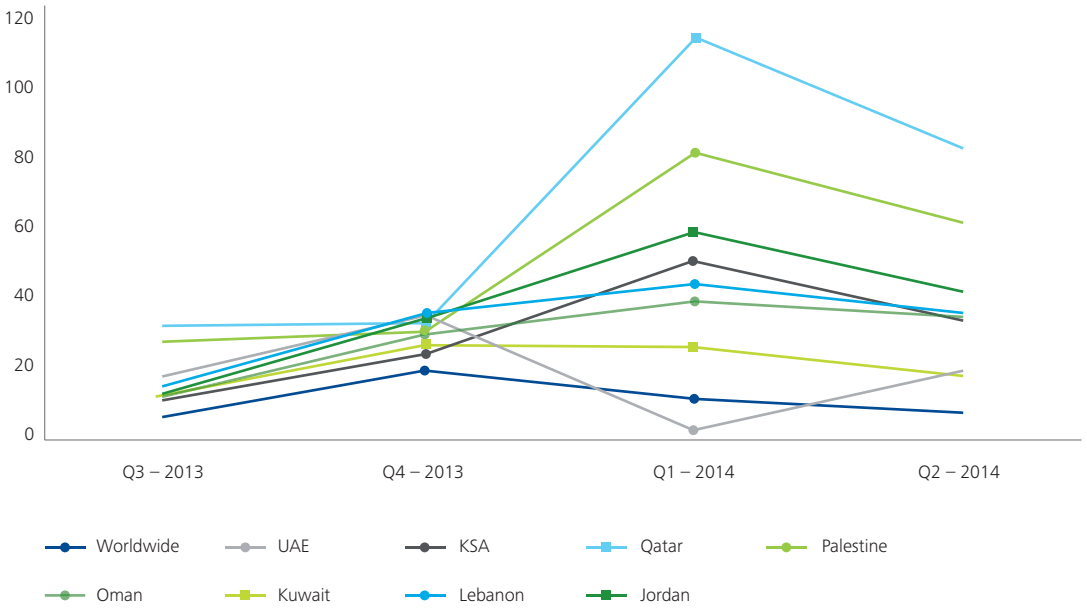
The Middle East, more specifically member states of the Gulf Cooperation Council (GCC), is perceived as a region of economic wealth. To cyber criminals who are trying to exploit governments, public and private institutions for financial gains, this makes the Middle East a central target for attack and indeed has been.

In short, the strategic things you do to grow your business or achieve your mission are at the heart of the cyber risks your organization faces

Above average malware infection rates

Since 2012, every country in the Middle East has had, almost without exception, at least double (and in some cases ten times) the number of infected systems than the global average as per Microsoft's quarterly report on the average malware infection rate per country (see chart below).

Average malware infection rate per country



Source: Microsoft

It becomes clear that protecting everything–while perhaps not impossible–would be economically impractical and would likely impede some of your most important strategic initiatives

Two questions arise: what are the underlying reasons for this trend and how can organizations actually reverse it to start winning the cyber risk battle?

The first question depends a lot on the organization itself. Over the past two decades, we have woven a fabric of always connected, always on in our economy and society via the Internet–a platform that was designed primarily for sharing information, not protecting it.

Your organization, whether functioning in the public or private sector, has no doubt benefitted from this connectivity–driving innovation, efficiency, and performance that were unthinkable a generation ago. You've likely used it to transform relationships with customers, build new revenue streams, or overcome geographic constraints. Or perhaps it has enabled you to gather data that shape your market strategy, accelerate the launch of products and services, or automate diverse operational systems.

You have probably also extended your capabilities through outsourcing, partnering, and the use of contractors, or engaged in reorganization, mergers, acquisitions, and divestitures. With that said, this increasing digital reach has added layers of complexity, volatility, and dependence on infrastructure not fully within your control. Your efforts to grow, serve, differentiate and streamline introduce new gaps and opportunities that attackers will try to exploit–because your adversaries, too, leverage the Internet to accomplish much more, much faster, and from anywhere. In short, the strategic things you do to grow your business or achieve your mission are at the heart of the cyber risks your organization faces.

When we consider this inherent link between business performance, innovation and cyber risk, it becomes clear that protecting everything–while perhaps not impossible–would be economically impractical and would likely impede some of your most important strategic initiatives.

Which brings us to the second question and the central theme of this article. If protecting everything is economically impractical then what should you be protecting? And at what level of investment?

In the interest of helping organizations answer these and other questions, members of the World Economic Forum's Partnering for Cyber Resilience initiative recently proposed a conceptual framework for measuring the impact of, and exposure to, cyber threats. Known as cyber value-at-risk, the model provides a starting point for quantifying cyber risk, ultimately allowing executive leaders to make more informed, confident decisions about their organization's risk tolerances and thresholds, cyber security investments, and other risk mitigation and transfer strategies.

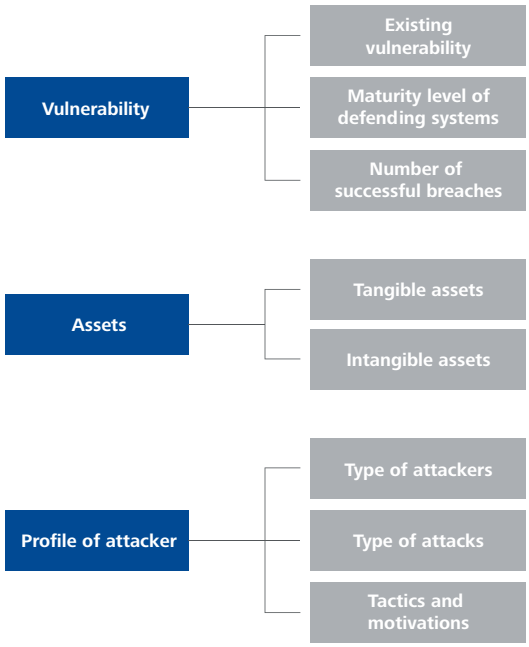
Cyber value-at-risk

The concept of cyber value-at-risk is based on the notion of value-at-risk (VaR), which seeks to express the risk of loss over a specific period of time. Similarly, cyber value-at-risk seeks to use probabilities to estimate likely losses from cyber attacks during a given time frame.

Cyber value-at-risk considers three components of cyber risk:

1. The vulnerability profile
2. The assets
3. The profile of attackers and the potential threat actors to an organization.

Cyber value-at-risk components



Source: World Economic Forum, "Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats"

Vulnerabilities take into consideration the number of unpatched systems inside an organization, the number of previous compromises it has experienced, and the maturity level of its defending systems as defined by the number of security updates applied, the number of defensive software components installed on the network, and the network typology and infrastructure.

Assets vary by organization, but on the tangible side they typically include funds and financial instruments, infrastructure, production facilities, and financial losses incurred through temporary business disruption, complete business interruption, and regulatory fines. On the intangible side, assets frequently encompass intellectual property (IP), customer or employee data, and a company's reputation.

Attacker profile looks at the type of threat actors, whether they're amateurs, state-sponsored, or part of organized crime rings; their motivations (e.g. financial gain, theft of trade secrets, destruction, reputation damage); and the sophistication of the attacks they tend to perpetrate.

While still a work in progress, the next steps for the cyber value-at-risk framework is applying real-world data to the model. The hope is that exposing the potential benefits of cyber value-at-risk will prompt industry participants to share more of the data needed to make the model work effectively. In the meantime, cyber security leaders at their organizations can use the notion of risk-based quantification, in tandem with a Secure.Vigilant.Resilient™ approach to cyber risk mitigation, to position themselves to use the cyber value-at-risk model and justify budget requests to the executive team and board.

by **Fadi Mutlak**, Partner, Cyber Security Leader, Deloitte Middle East