Deloitte.

Cyber Security

Digital Nightmare

Burç Yıldırım

Cyber risks are not new, so what's different?

- Small, highly skilled groups exact damage
- Attackers often have very specific motives (information theft, disruption, notoriety)
- They're spread across the globe, often beyond the reach of law enforcement
- Threat velocity is increasing, response window is shrinking

Complexity and volume of threats is increasing

Potential for physical and economic damage

The evolving threat landscape…

Lilly scientists **stole $55 million in trade secrets**[1]
Indianapolis Business Journal, October 8, 2013

$55 million

Last year, over **800 million records were breached globally**, up from 250 million in 2012
The Economist, July 2014

800 million

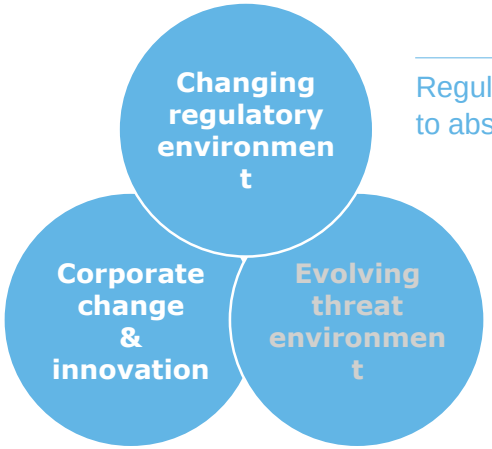
Target missed signs of a data breach (**40 million credit card numbers compromised**)[2]
NY Times, March 13, 2014

40 million

On a scale of 1 to 10…**American preparedness** for a **large-scale cyber attack** is around a **3**[3]
NY Times, July 2012

3

Why?



Regulatory changes continue to absorb resources and attention.

Technology innovations that drive business growth also create cyber risk. New technology-enabled business models create new opportunities for malicious actors to exploit and higher likelihood of accidental vulnerabilities.

Cyber threats are asymmetrical risks. Cyber crime grows in sophistication, and attacks increase in speed and number, while time to respond decreases. Targeted attacks on operations, brand, and competitive advantage are more impactful than ever.

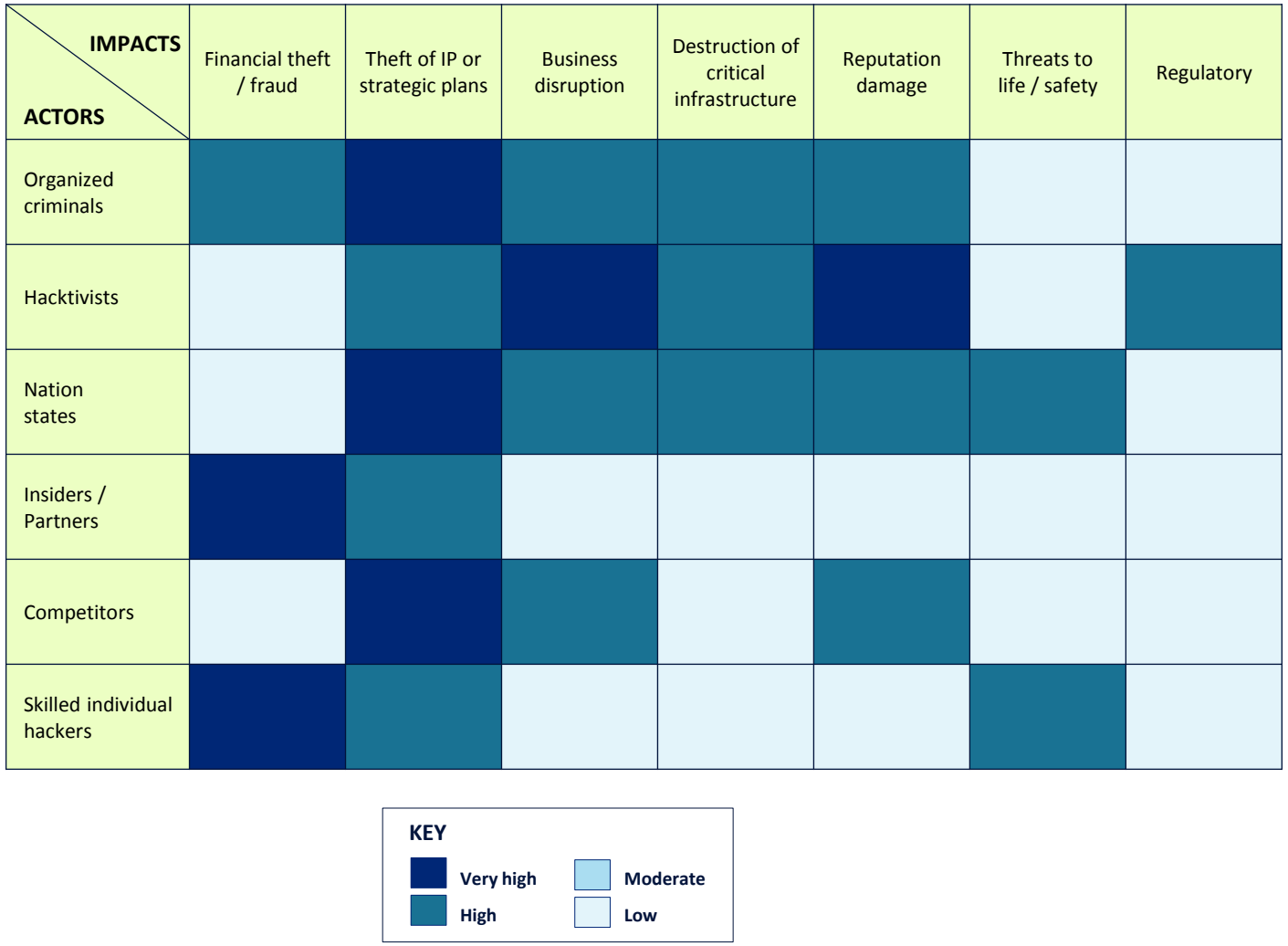
1 http://www.ibj.com/lilly-employees-stole-55-million-in-trade-secrets-indictment-alleges/PARAMS/article/43949
2 http://www.nytimes.com/2014/03/14/business/target-missed-signs-of-a-data-breach.html?_r=0
3 http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html?_r=0

Threat actors and their motives vary by industry and organization

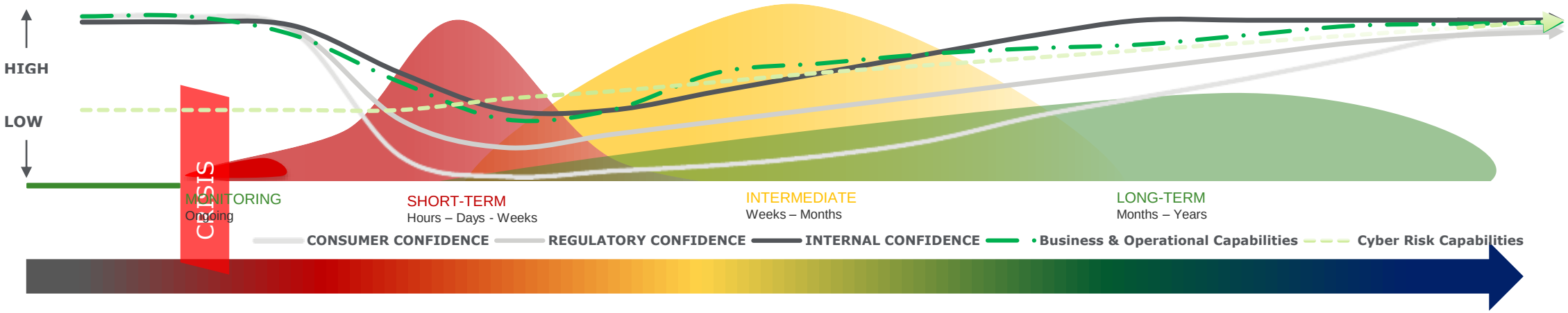
A typical cyber risk heat map for the Process & Industrial Products sector

Notable insights:

- Criminals are seeing the supply chain as a means of accessing information they wouldn't otherwise be able to get from a large, proficiently run, well secured global organization.
- Attacks are no longer ‘smash and grab' but focused on maintaining hidden presence for years to access what makes the organization competitive (e.g., manufacturing processes, unique supply chain methods, marketing strategies, research and development, etc.).
- Manufacturing plants and distribution centers utilize critical infrastructure to process the production of goods and coordinate the supply chain. Emerging threats exist to attack critical assets and disrupt business operations.



Cyber incident response lifecycle
The interplay between capabilities and stakeholder confidence



At the most strategic level, recovering from a cyber incident involves an important balance between recovering or enhancing *capabilities* and restoring *confidence* among a broad spectrum of stakeholders.

Capabilities

- *Business and operational capabilities* need to be restored in the case of disruptive or destructive attacks, which usually takes hours or days, but can extend for weeks or even months in severe cases.
- *Cyber risk capabilities* need to be enhanced to secure the environment, provide better visibility into ongoing threats, and reduce the impact of future attacks. Important progress can be made in the short term, but significant improvement usually takes months or years to achieve.

Confidence

- *Customers* are most immediately concerned with direct personal damage from loss of data, but may develop longer-term brand aversion
- *Employees* can be overwhelmed by negative publicity and increased chaos in both their work and personal lives
- *Business partners* are concerned about the immediate threat of cross contamination and the longer-term integrity of business transactions
- *Regulators* are concerned about consumer protection, existential threats to the business, and the broader soundness of the industry
- *Capital markets and shareholders* are highly attuned to potential impacts to revenue and earnings in the near term and the viability of the brand over a longer time horizon. They pay a lot of attention to the attitudes of other stakeholders, especially customers and regulators.

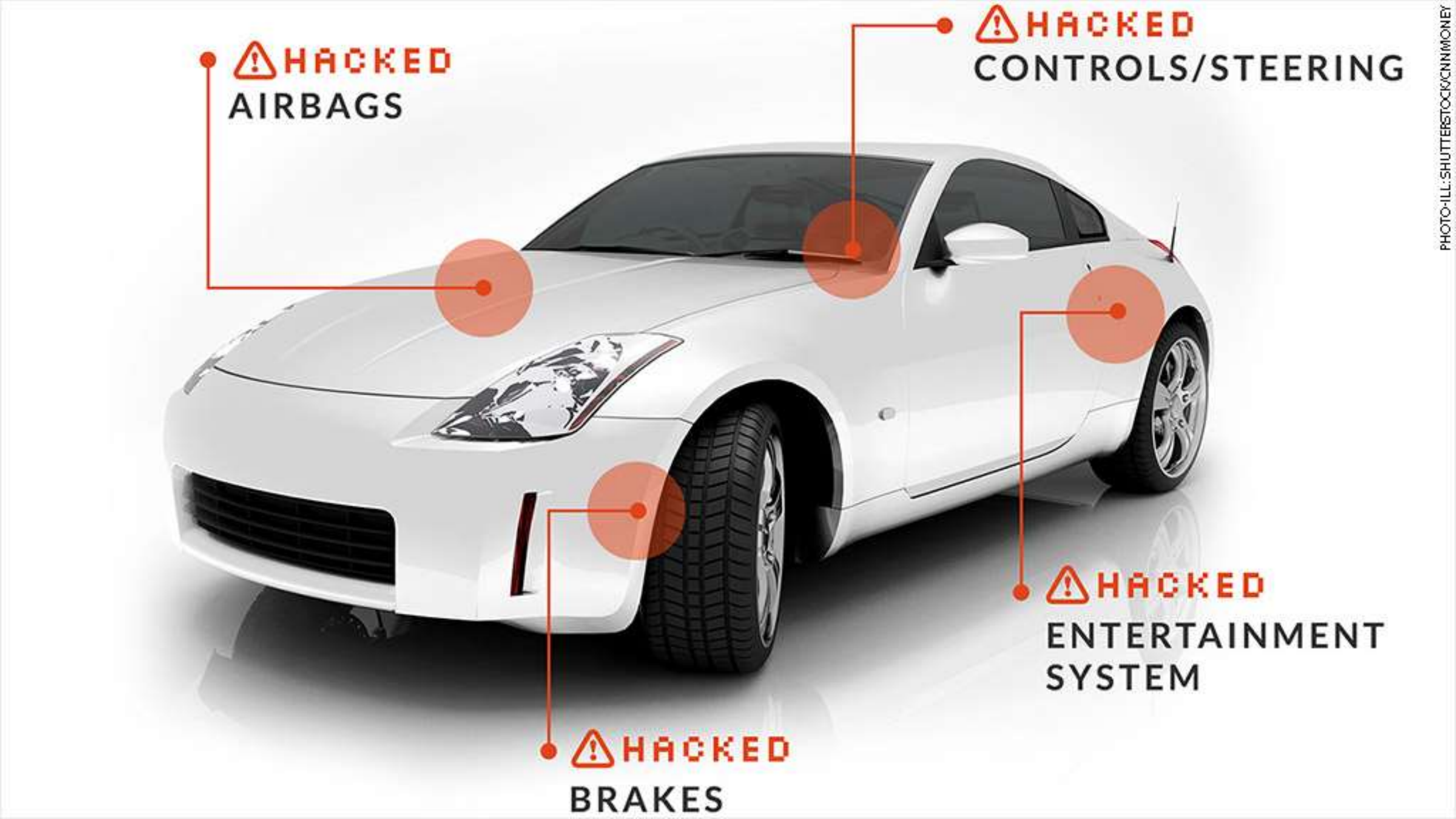

TARGET

]HackingTeam[

Rely on us.

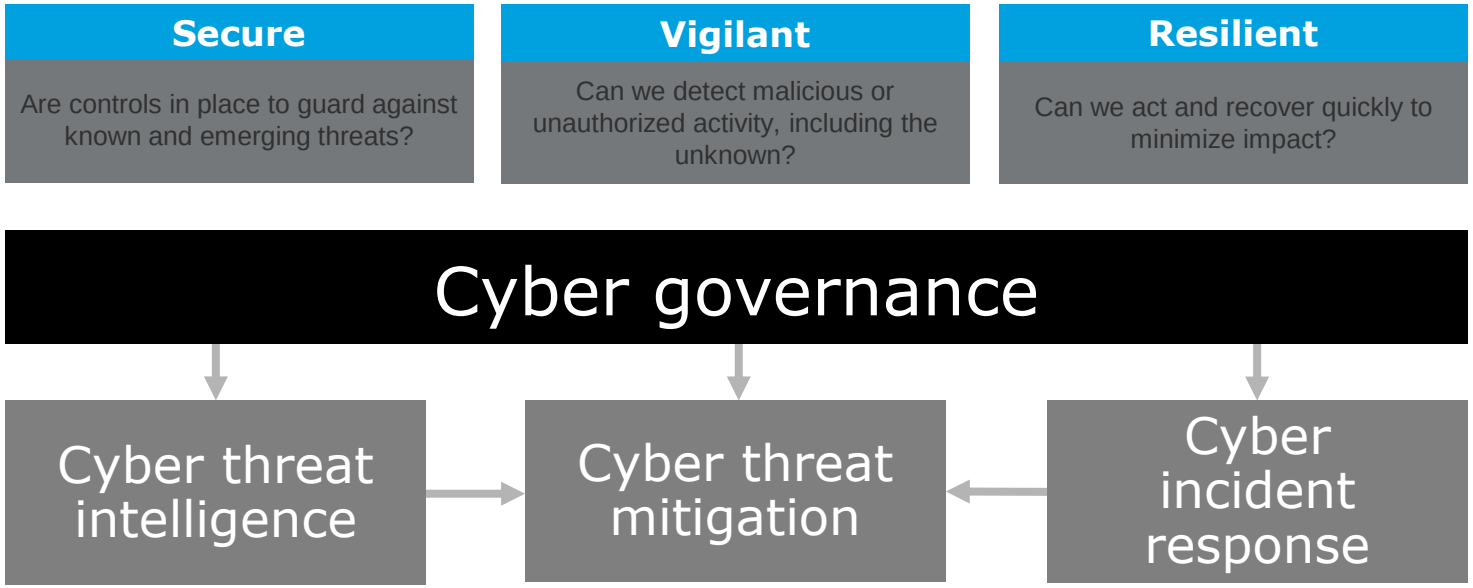
Name	Country	Name	Maintenance	Status
AFP	Australia	Australian Federal Police	-	Expired
AZNS	Azerbaijan	Ministry of National Defence	6/30/2015	Active
BHR	Bahrain	Bahrain	5/5/2015	Not Active
PHANTOM	Chile	Policia de Investigation	12/10/2018	Delivery scheduled (end of november)
MDNP	Colombia	Policia Nacional Intelligencia	10/30/2016	Active
SENAIN	Ecuador	Seg. National de intelligencia	10/30/2016	Active
GNSE	Egypt	Min. Of Difence	12/31/2014	Active
INSA	Ethiopia	Information Network Security Agency	10/31/2015	Active
HON	Honduras	Hera Project - NICE	4/30/2015	Active
INTECH-CONDOR	K Iraqi	Kurdistan Iracheno	6/30/2015	Active
KNB	Kazakistan	National Security Office	12/31/2014	Active
MACC	Malaysia	Malaysia AntiCorruption Commission	1/31/2014	Expired
MIMY	Malaysia	Malaysia Intelligene	12/31/2014	Active
PMO	Malaysia	Prime Minister Office	3/31/2015	Active
CUSAEM	Mexico	Police	-	Expired
DUSTIN	Mexico	Durango State Government	11/30/2015	Active
EDQ	Mexico	Queretaro State Government	3/31/2014	Expired
GEDP	Mexico	Puebla State Government	7/31/2014	Expired
MCDF	Mexico	Mexico Police	-	Expired
MXNV	Mexico	Mexico Navy	-	Expired
PEMEX	Mexico	Army Mexico	3/31/2015	Not Active
PF	Mexico	Policia Federal	-	Expired
PGJEM	Mexico	Procuradoria General De Justicia	12/31/2014	Active
SDUC	Mexico	Campeche State Governement	6/30/2014	Expired
SEGOB	Mexico	Seg. National de Gobernacion (CISEN)	12/31/2014	Active
SEPYF	Mexico	State Government Baja California	9/21/2015	Active
SSPT	Mexico	TaumalipasState Government	7/20/2015	Active
YUKI	Mexico	Yucatan State Government	11/30/2015	Active
MOACA	Mongolia	Ind. Authoirty Anti Corruption	6/3/2015	Active
ALFAHAD-PROD	Morocco	Minister of Interior	12/31/2014	Active
CSDN-01	Morocco	Intelligence Agency	12/31/2014	Active


MIRAI


HACKED
AIRBAGS
HACKED
CONTROLS/STEERING
HACKED
ENTERTAINMENT SYSTEM
HACKED
BRAKES
PHOTO-ILL: SHUTTERSTOCK/CNNMONEY

Building a resilient cyber security organization

This means having the **agility to prevent, detect and respond** quickly and effectively, not just to incidents, but also to the consequences of the incidents



Deloitte.