RSA Conference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: GRC-W04

When attackers want your IP: Valuing and guarding prized business assets

Emily Mossburg

Advisory Cyber Risk Services

J. Donald Fancher

Advisory Financial Transactions

#RSAC

The IP cyber theft landscape

Trends fueling IP cyber theft

- Digitization of everything
- Connection of everyone and everything to the internet
- Expanding ecosystems – even R&D is outsourced
- New technologies, such as 3D printing, continue to introduce new forms and vehicles for IP theft
- In a competitive economic landscape, stealing IP is easier and faster than creating it

44% of executives named loss of IP or strategic proprietary information as one of their top three cyber risk concerns.*

The issue receives growing law enforcement and policy attention.

Many types of IP – and theft across many industries

Automotive

- Employee steals trade secrets to foreign competitor for personal gain

Industrial products

- Former employee steals formulas, raw materials information, sales and cost data, product research, marketing data and other IP before gaining employment at a competitor

Energy & resources

- Foreign nationals indicted for stealing designs, financial information, attorney-client privileged communications and other IP from energy product manufacturers

Financial services

- Programmer steals software code owned by a third party

Life sciences

- Scientists charged with stealing employer’s biomedical information for resale overseas

Media and entertainment

- Cybercriminals plead guilty to conspiracy for stealing unreleased software, source code, and copyrighted materials

Federal government

- Foreign nationals hacked systems to steal manufacturing plans

Information gathered from https://www.fbi.gov/collections/intellectual-property-theft

Are organizations adequately addressing the impact of IP theft?

Cyber programs tend to be shaped based on known threats and vulnerabilities

- Security controls, detection capabilities, and incident response plans are largely based on the risks associated with volumes of sensitive data records

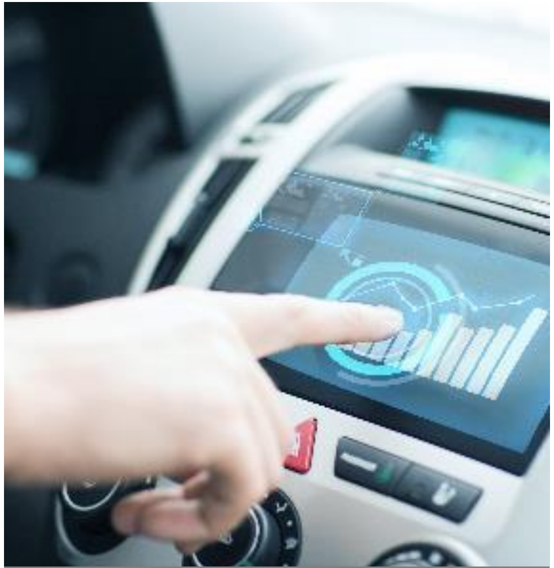
Organizations expect certain well-known impacts

- Financial
- Regulatory
- Reputational

COMMONLY ASSOCIATED COSTS

- Customer breach notification
- Post-breach customer protection
- Regulatory compliance costs
- Public relations costs
- Attorney fees and litigation
- Cybersecurity improvements

What is the broader impact of an attack aimed at undermining competitive advantage?

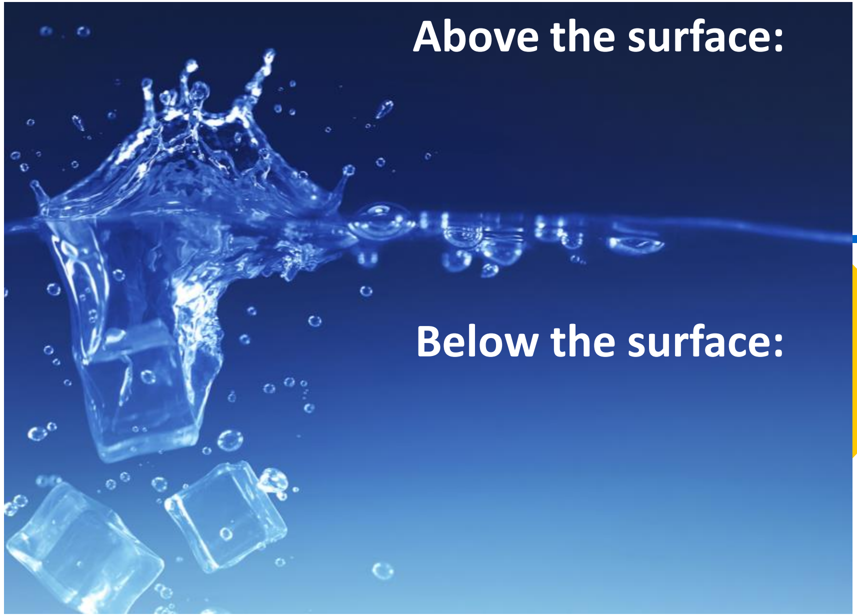


Supply chain tampering…

Disruption of critical services…

Theft of strategic information…

A narrow lens on cyberattacks can leave organizations unprepared for the broader potential costs

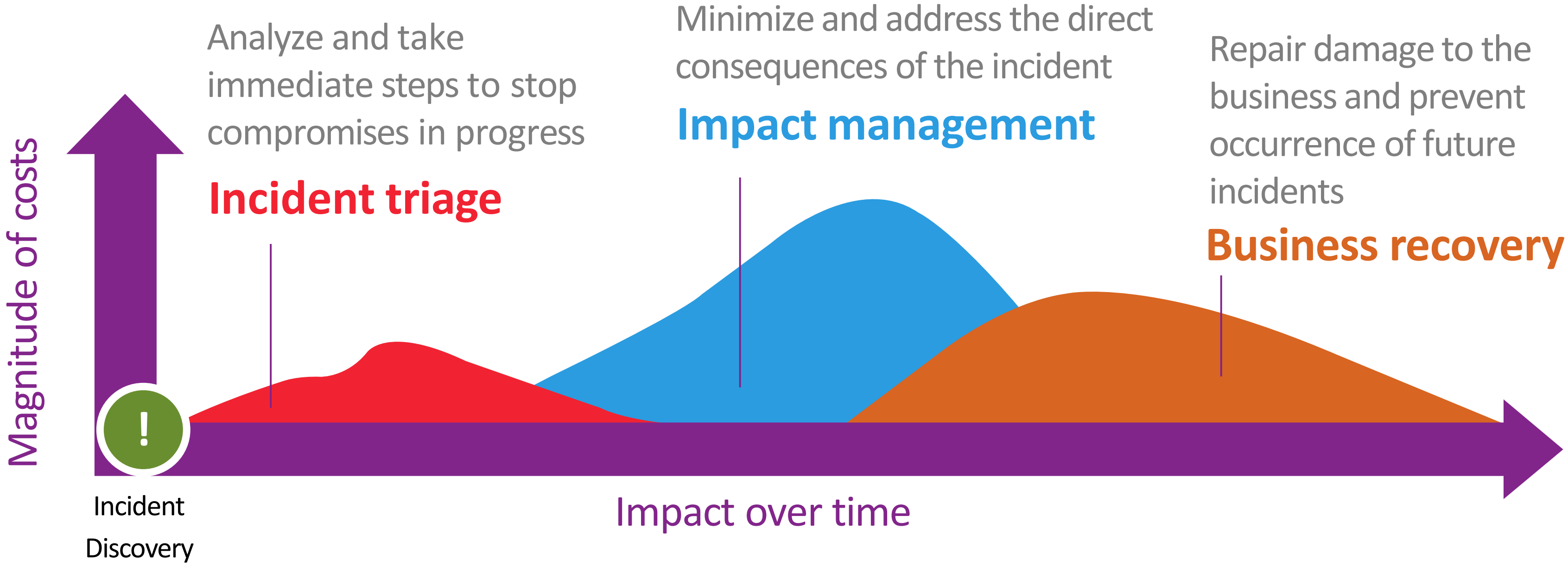


- Customer breach notification
- Post-breach customer protection
- Regulatory compliance costs
- Public relations costs
- Attorney fees and litigation
- Cybersecurity improvements

- Impact to current contracts
- Devaluation of trade name
- Loss of IP
- Cost of lost customers
- Impact of operational disruption and/or destruction
- Insurance premium increases
- Increased cost to raise debt

…and unprepared for the duration of recovery efforts

Costs are incurred and impacts are felt over years, in several phases



Analyze and take immediate steps to stop compromises in progress
Incident triage
Minimize and address the direct consequences of the incident
Impact management
Repair damage to the business and prevent occurrence of future incidents
Business recovery
Magnitude of costs
!
Incident Discovery
Impact over time

Illustrating a case of IP cyber theft

A fictitious technology company

$40B Revenue

Growth rests on innovative products to support management of Internet of Things (IoT) devices

Pay $3.75M annually for $150M in cyber insurance

60,000 employees

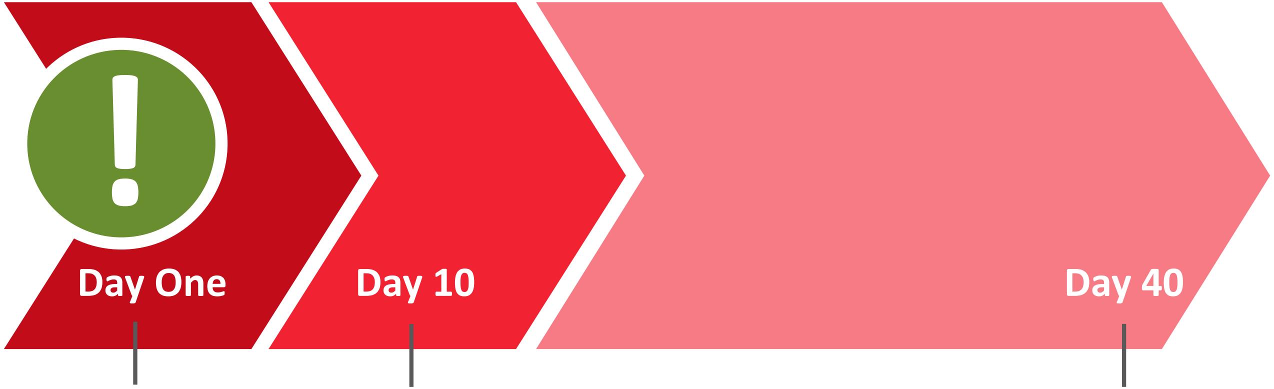
Hundreds of contracts across many industries, including some very large government contracts

Relatively mature incident response capabilities

Anatomy of the attack they face

In six months, the tech company plans to launch a new version of a core networking product

This product line is expected to yield 50% of the company's revenue over the next five years



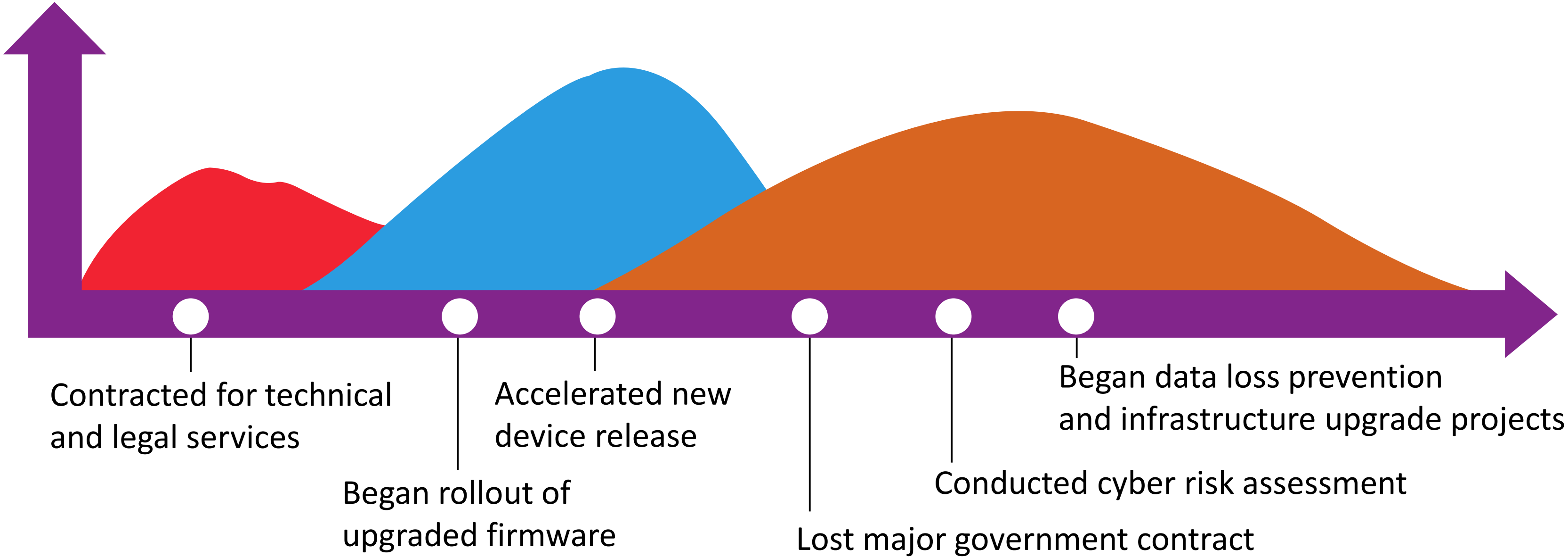
Day One: A federal agency notifies the company that its infrastructure has been breached by a foreign nation-state

Day 10: An investigation shows that IP tied to 15 out of 30 product lines was stolen

Day 40: A tech blog reveals that the foreign entity is reverse-engineering the product that is due to be launched

Recovering from the rippling effects

- Sales of many products are suspended
- A major contract is lost
- Margins and operating efficiency decline
- Unplanned legal, public relations, and product development costs
- Development plans are accelerated



Contracted for technical and legal services

Began rollout of upgraded firmware

Accelerated new device release

Lost major government contract

Conducted cyber risk assessment

Began data loss prevention and infrastructure upgrade projects

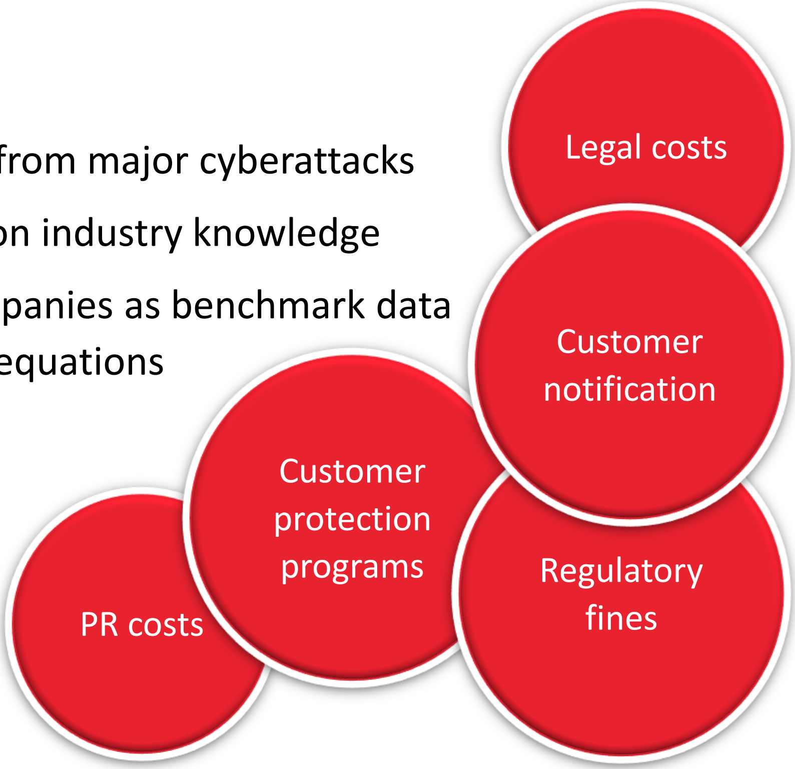
Estimating financial impact of the attack

Deriving cost and duration data

- Leveraged experience helping companies recover from major cyberattacks
- Developed fictitious profiles and scenarios based on industry knowledge
- Used publicly available information on similar companies as benchmark data to derive factors used in direct cost and valuation equations

Calculating direct costs

- Relatively simple to approximate based on publicly available information
- Leveraged existing studies



Legal costs

Customer notification

Customer protection programs

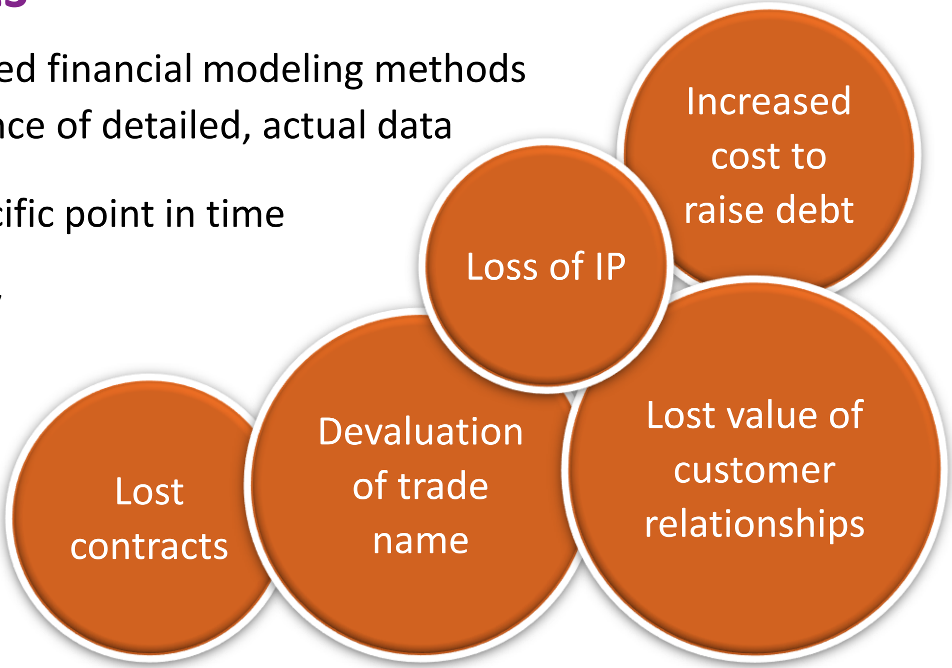
Regulatory fines

PR costs

Modeling potential cyberattack impact

Calculating intangible impacts

- Applying professional judgement, accepted financial modeling methods and reasonable assumptions in the absence of detailed, actual data
- Financial impact is associated with a specific point in time
- With-and-without / But-for methodology
- Relief-from-royalty methodology
- Reliance on assumptions


Increased cost to raise debt
Loss of IP
Lost contracts
Devaluation of trade name
Lost value of customer relationships

What does it cost?

Total potential impact >$4B

- Many of the costs commonly associated with PII-type data breaches do not factor in
- Greatest impacts are intangible costs
- The value of lost IP is not the major cost, but the theft of IP has rippling impacts

	Cost Factors	Cost (Mil.)	% Total
Known costs	Customer breach notification	--	--
	Post-breach customer protection	--	--
	Regulatory compliance	--	--
	Public relations	$1.00	0.02%
	Attorney fees and litigation	$11.30	0.24%
	Cybersecurity improvements	$13.00	0.27%
Hidden costs	Insurance premium increases	$1.00	0.02%
	Increased cost to raise debt	--	--
	Operational disruption	$1,200.00	25.09%
	Lost value of customer relationships	--	--
	Value of lost contracts	$1,617.00	33.81%
	Devaluation of trade name	$1,697.00	35.48%
	Loss of intellectual property	$242.50	5.07%
	Total	**$4,782.80**	100.00%

Improving management of IP cyber risk: no need to start from scratch

✓ Creators of IP – researchers and scientists – understand what's at stake

✓ Cybersecurity programs have the foundational elements needed to protect their organizations from threats and vulnerabilities

Business leaders need to drive:

- Scenario planning based on business impacts
- Data inventory and classification
- More attention to insider threat programs

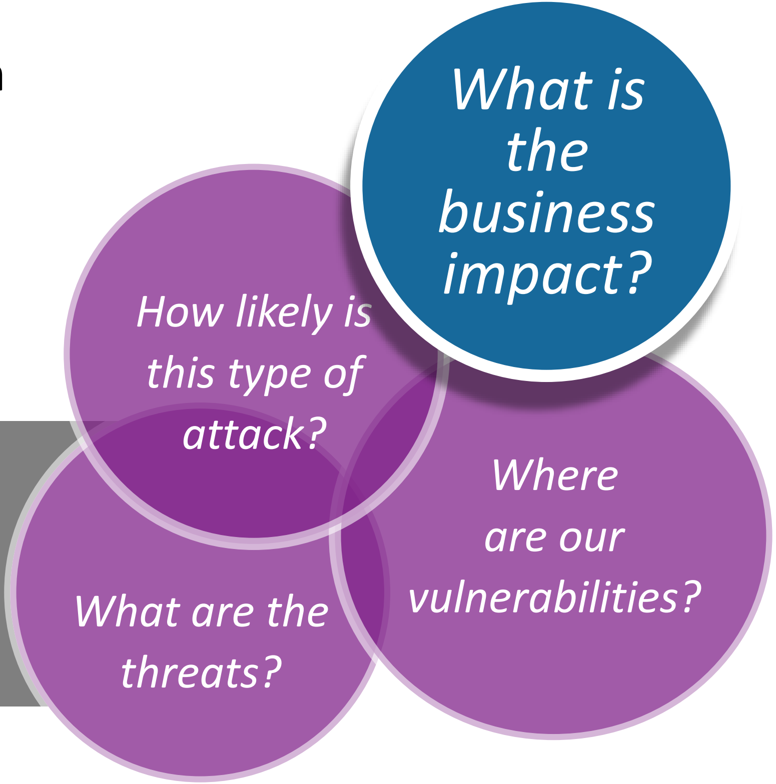
Building a data governance foundation is a huge effort – so big that many companies don't want to do it, or no one wants to own it

Bridging the gap and engaging business leaders

Cybersecurity programs continue to focus on the threats, vulnerabilities and probability

More attention should be paid to the true damages a particular cyberattack may cause

By looking realistically at the potential costs, business leaders can right-size investments to better protect their most valuable assets


What is the business impact?
How likely is this type of attack?
Where are our vulnerabilities?
What are the threats?

Questions?

Emily Mossburg
emossburg@deloitte.com
@EmilyJMossburg

J. Donald Fancher
dfancher@deloitte.com
@jdfancher