Management of Insider and Third-Party Risks

Prof. Kai-Lung Hui, HKUST Business School

Major Security Incidents

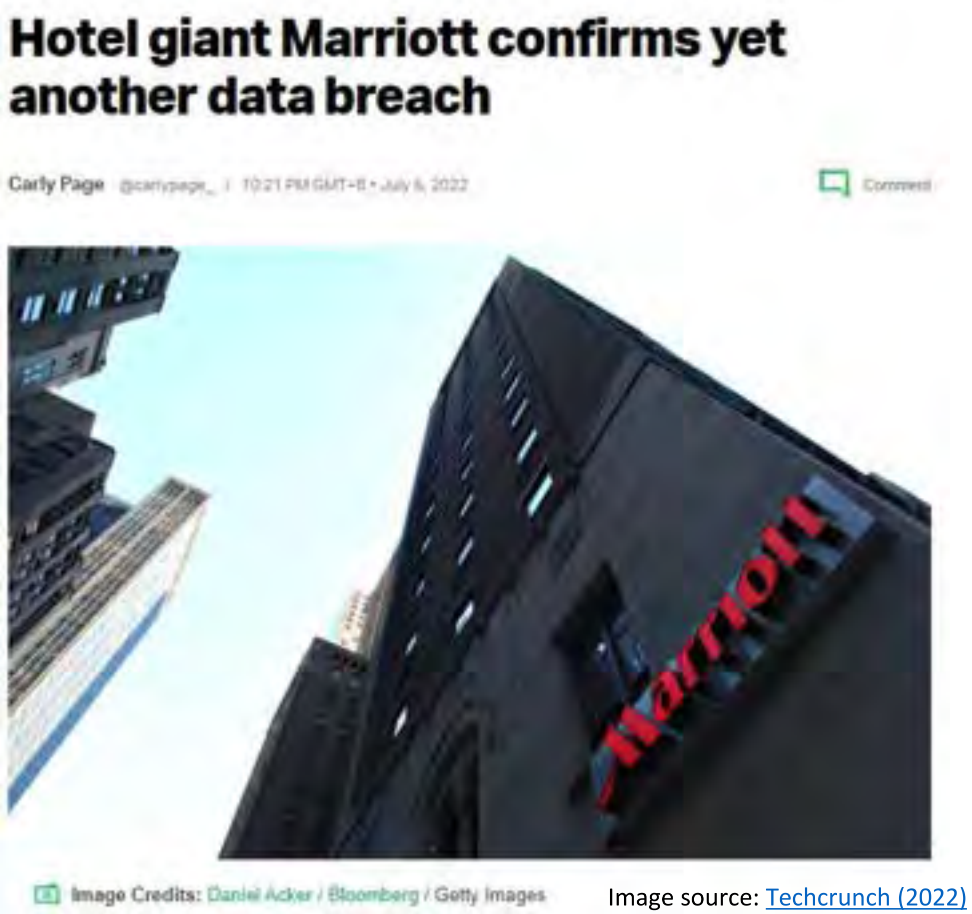


Image source: Techcrunch (2022)

Hotel group Marriott International has confirmed another data breach, with hackers claiming to have stolen **20 gigabytes of sensitive data, including guests' credit card information**…"Marriott International is aware of a threat actor who used **social engineering** to trick one associate at a single Marriott hotel into providing access to the associate's computer…The threat actor did not gain access to Marriott's core network."

…Samples of the data provided to Databreaches.net purport to show reservation logs for airline crew members from January 2022 and names and other details of guests, as well as credit card information used to make bookings.

…**Hackers breached the hotel chain in 2014 to access almost 340 million guest records worldwide** — **an incident that went undetected until September 2018** and led to a £14.4 million ($24 million) fine from the U.K.'s Information Commissioner's Office. **In January 2020, Marriott was hacked again in a separate incident that affected around 5.2 million guests.**

Major Security Incidents

HKUST BUSINESS SCHOOL 香港科大商學院 WORLD CLASS IN ASIA

Alibaba execs hauled in to discuss Shanghai Police data leak

Plus: Weibo cracks down on political puns; Singaporean crypto biz Vauld restructures; Philippines fights Facebook rumors

Laura Dobberstein — Mon 18 Jul 2022 // 01:15 UTC

2

ASIA IN BRIEF Senior execs from Alibaba Cloud were summoned to discuss the data leak that saw information pertaining to a billion Chinese citizens sold on the dark web, according to Nikkei and *The Wall Street Journal*.

The leak is thought to have come from a misconfigured Alibaba Cloud server that did not require a password to access the trove, which exposed names, home addresses, ID numbers, phone numbers, and criminal records.

Cyber security researchers have also alleged the digital certificates had expired – perhaps four years previously.

Since the discovery of the leak, Alibaba engineers have reportedly been ordered to review database architectures it offers in its cloud, and to check configurations used by other clients.

Image source:
The Register (2022)

Recent Incident

HKUST BUSINESS SCHOOL 香港科大商學院
WORLD CLASS IN ASIA

Colonial Pipeline paid $5 million ransom to hackers

PUBLISHED THU, MAY 13 2021·2:05 PM EDT | UPDATED THU, MAY 13 2021·6:38 PM EDT

Eamon Javers @EAMONJAVERS | Amanda Macias @AMANDA_M_MACIAS

SHARE

KEY POINTS

- Colonial Pipeline paid a ransom to hackers after the company fell victim to a sweeping cyberattack, one source familiar with the situation confirmed to CNBC.
- A U.S. official, who spoke on the condition of anonymity, confirmed to NBC News that Colonial paid nearly $5 million as a ransom to the cybercriminals.
- It was not immediately clear when the transaction took place.

"Last week's assault, carried out by a criminal cybergroup known as DarkSide, forced the company to shut down approximately 5,500 miles of pipeline, leading to a disruption of nearly half of the East Coast fuel supply and causing gasoline shortages in the Southeast…

Criminals behind these types of cyberattacks typically demand a ransom in exchange for the release of data."

Source: CNBC

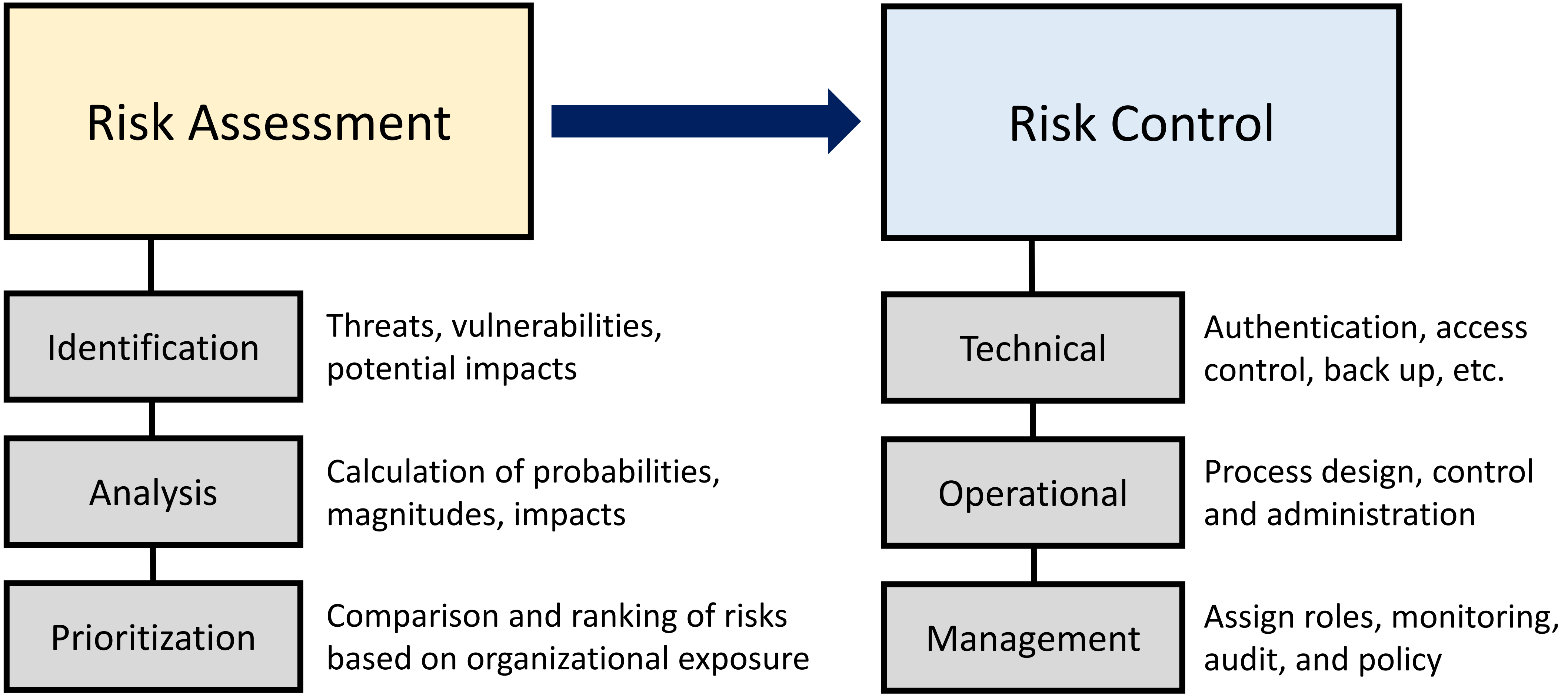
Key Questions

- How did these breaches or leakages happen?
- Are you vulnerable to these attacks?

Risk Management

- The process of identifying vulnerabilities and taking careful steps to protect the business
  - Confidentiality, integrity, availability
  - Internal and external threats

Typical Risk Management Process



Exemplary Attack: FCB Taiwan

Hackers steal millions from ATMs without using a card

by Ivana Kottasova

Taiwan is trying to figure out how hackers managed to trick a network of bank ATMs into spitting out millions.

Source: CNN

“They didn't use bank cards but rather appeared to gain control of the machines with a "connected device," possibly a smartphone, the police said in a statement Thursday. Authorities are now hunting the thieves, who they say came from Russia and eastern Europe.

The ATMs were made by German manufacturer Wincor Nixdorf (WNXDY). The company confirmed that several of its machines in Taiwan were hacked in a "premeditated attack."

Wincor Nixdorf said Thursday it had sent security experts to support local investigators in Taiwan.

Prosecutors said the machines were infected with three different malware files that instructed them to "spit out cash" and then deleted evidence of the crime. They described the case as the first of its kind in Taiwan. Wincor Nixdorf said it has no evidence that the malware was introduced into the network via the ATMs themselves.”

Exemplary Attack: Target

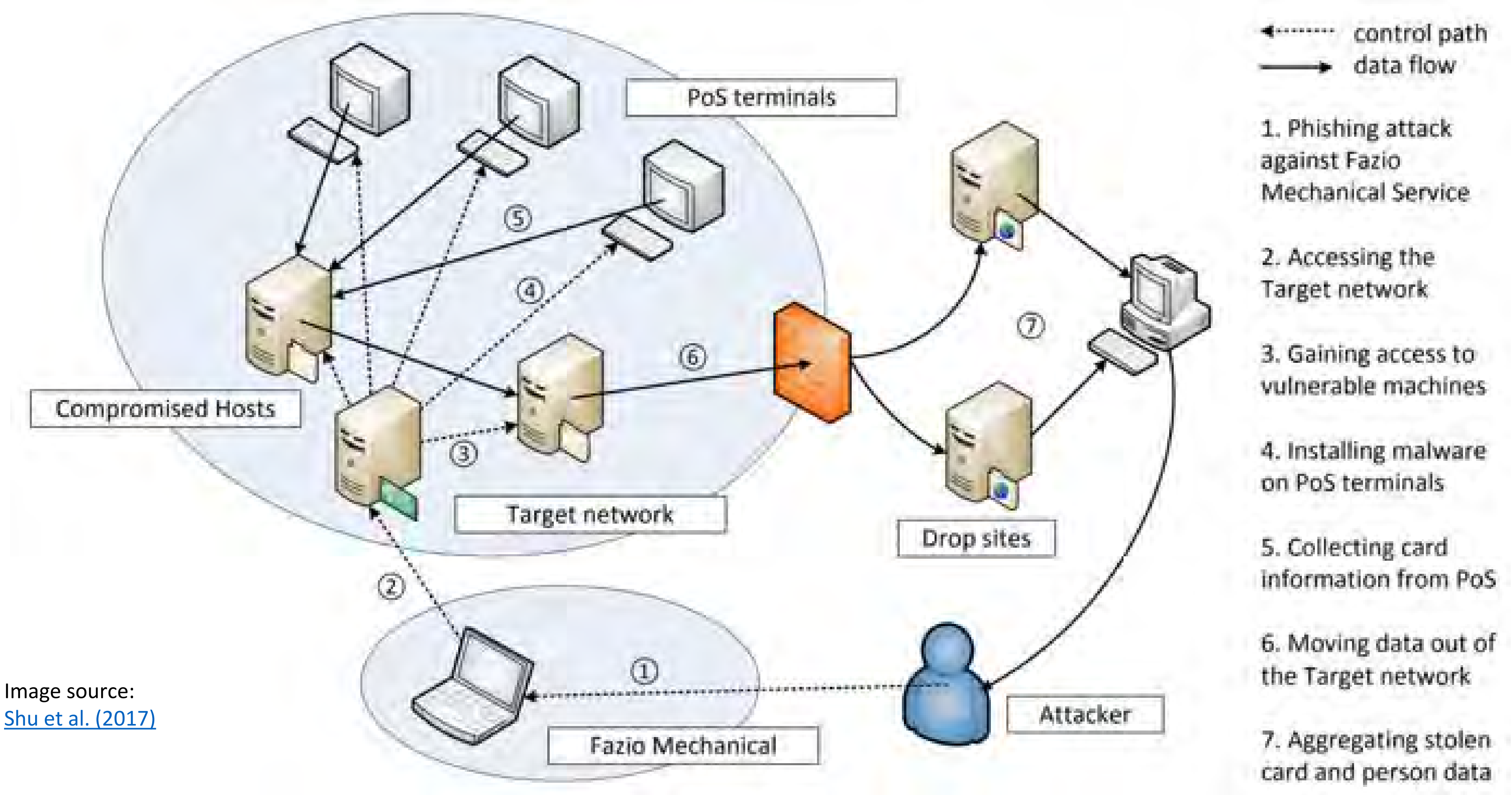


Image source:
Shu et al. (2017)

Food For Thought

- What have these organizations missed? Does risk management address their risks?

Case: Password Analysis

ID	Name	Passw. routine	Accounts with passw.	Leak date
1	000webhost.com	$p	15 035 687	≈ Mar. 2015
2	17.media	md5($p)	3 824 575	≈ Sep. 2015
3	51cto.com	md5(md5($p).$s), md5($p)	3 923 449	≈ Dec. 2013
4	7k7k.com	$p	9 231 185	≈ Oct. 2011
5	aipai.com	md5($p)	4 529 928	≈ Apr. 2011
6	ashleymadison.com	bcrypt($p)	36 140 796	≈ July 2015
7	badoo.com	md5($p)	122 730 419	≈ June 2016
8	csdn.net	$p	6 425 905	≈ Oct. 2011
9	duduniu.cn	$p	14 192 866	≈ Aug. 2011
10	gawker.com	des($p)	487 292	≈ Dec. 2010
11	gmail.com	$p	4 925 994	≈ Sep. 2014
12	imesh.com	md5(md5($p).$s)	51 308 651	≈ Sep. 2013
13	ispeak.cn	$p	8 294 278	≈ Apr. 2011
14	linkedin.com	sha1($p)	112 275 414	≈ Feb. 2012
15	mail.ru	$p	5 269 103	≈ Sep. 2014
16	mate1.com	$p	27 402 581	≈ Feb. 2016
17	mpgh.net	md5(md5($p).$s)	3 119 180	≈ Oct. 2015
18	myspace.com	sha1($p)	358 986 419	≈ 2008
19	naughtyamerica.com	md5($p)	989 401	≈ Apr. 2016
20	nexusmods.com	md5(md5($s).md5($p))	5 918 540	≈ Dec. 2015
21	r2games.com	md5(md5($p).$s), md5($p)	11 758 232	≈ Oct. 2015
22	renren.com	$p	4 392 208	≈ Nov. 2011
23	sprashivai.ru	$p	3 472 645	≈ May 2015
24	taobao.com	$p	14 769 995	≈ Jul. 2015
25	tianya.cn	$p	29 642 564	≈ Nov. 2011
26	twitter.com	$p	26 121 984	≈ June 2016
27	vk.com	$p	92 144 526	≈ 2012
28	weibo.com	$p	4 529 994	≈ Dec. 2011
29	xiaomi.com	md5(md5($p).$s)	8 281 358	≈ May 2014
30	xsplit.com	sha1($p)	2 990 112	≈ Nov. 2013
31	yandex.ru	$p	1 186 565	≈ Sep. 2014
Total accounts with email addr.: 994 301 846, **Total distinct email addr.:** 884 460 979				

Table 1: Analyzed identity leaks ($p - clear password, $s - salt)

Hash routine	Common name	# of leaks	# of dumps
$p	cleartext	16 (≈ 51.6%)	6 (≈ 28.5%)
md5($p)	MD5	4 (12.9%)	4 (≈ 19.0%)
sha1($p)	SHA-1	3 (9.7%)	3 (≈ 14.3%)
des($p)	descrypt	1 (≈ 3.2%)	1 (≈ 4.8%)
md5(md5($p).$s)	vBulletin-Hash	5 (≈ 16.1%)	5 (≈ 23.8%)
md5(md5($s).md5($p))	MyBB-Hash	1 (≈3.2%)	1 (≈ 4.8%)
bcrypt($p)	bcrypt	1 (≈ 3.2%)	1 (≈ 4.8%)

Table 2. Password routines of all identity leaks

Source: Jaeger et al. (2016)

Table 3. Credentials with cleartext passwords and percentage of recovered encrypted password, - was used for cleartext only leaks

Name	Clear cred.	Rec.	Name	Clear cred.	Rec.
000webhost.com	15 035 687	-	mpgh.net	247 499	8%
17.media	2 709 893	71%	myspace.com	328 152 578	91%
51cto.com	2 228 479	67%	naughtyamerica.com	911 781	92%
7k7k.com	9 231 185	-	nexusmods.com	2 691 088	45%
aipai.com	2 221 875	49%	r2games.com	364 927	3%
ashleymadison.com	2 559 028	8%	renren.com	4 392 208	-
badoo.com	114 090 491	97%	sprashivai.ru	3 472 645	-
csdn.net	6 425 905	-	taobao.com	14 769 995	-
duduniu.cn	14 192 866	-	tianya.cn	29 642 564	-
gawker.com	439 449	90%	twitter.com	26 121 984	-
gmail.com	4 925 994	-	vk.com	92 144 526	-
imesh.com	15 908 834	32%	weibo.com	4 529 994	-
ispeak.cn	8 294 278	-	xiaomi.com	1 167 052	14%
linkedin.com	104 955 280	93%	xsplit.com	2 904 588	97%
mail.ru	5 269 103	-	yandex.ru	1 186 565	-
mate1.com	27 402 581	-			
Total cleartext cred.: 848 590 922, **Cleartext passwords:** 320 201 615					

Case: Password Analysis

Source: [Jaeger et al. (2016)]

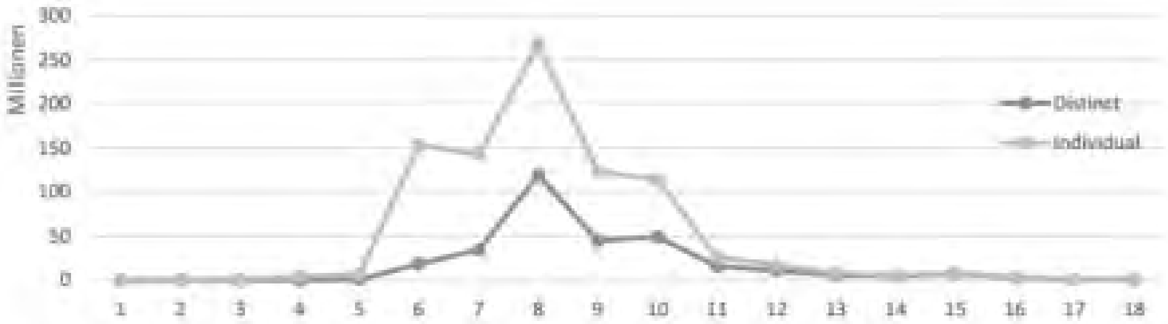


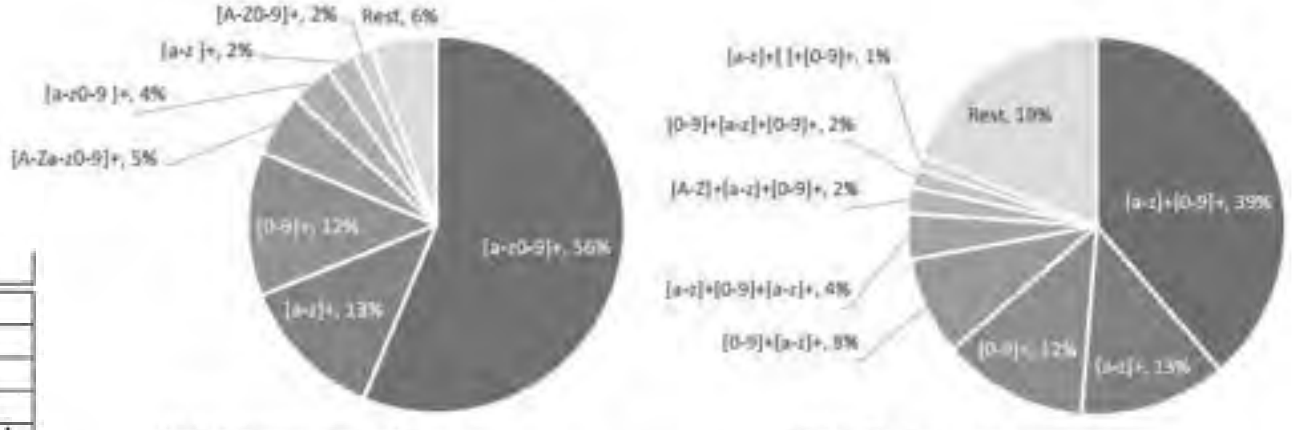
Fig. 2. Distribution of password lengths (distinct - each password only once, individual - password used by a user in a leaked source)

Table 4. Normalized top passwords

	Top 1-5		Top 6-10		Top 11-15		Top 16-20
1	123456	6	password	11	000000	16	abc123
2	111111	7	1q2w3e4r	12	1234567890	17	123qwe
3	12345678	8	1qaz2wsx	13	666666	18	654321
4	123456789	9	1234567	14	123321	19	112233
5	123123	10	iloveyou	15	qwerty	20	11111111

Table 5. Country-specific passwords

ID	Domain	Language	number of addresses	Top 5 passwords
1	.uk	British English	18 604 736	liverpool, arsenal, chelsea
2	.fr	French	32 207 859	azerty, marseille, doudou
3	.de	German	15 401 823	passwort, ficken, qwertz
4	.it	Italian	21 856 935	juventus, andrea, francesco
5	.nl	Dutch	3 513 385	welkom, welkom01, wachtwoord
6	.cn	Chinese	12 213 153	5201314, woaini, 1314520
7	.ru	Russian	119 002 753	qwertyuiop, UsdopaA, 1q2w3e4r5t



(a) Character classes (b) Character sequences

Fig. 3. Used characters in distinct passwords

Case: Password Analysis

ID	Source	ID	Source
1	000webhost.com	12	mpgh.net
2	17.media	13	myspace.com
3	51cto.com	14	naughtyamerica.com
4	aipai.com	15	nexusmods.com
5	ashleymadison.com	16	r2games.com
6	badoo.com	17	sprashivai.ru
7	csdn.net	18	tianya.cn
8	gawker.com	19	vk.com
9	imesh.com	20	xiaomi.com
10	linkedin.com	21	xsplit.com
11	mate1.com		

1	-																				
2	22.1	-																			
3	18.7	44.5	-																		
4	23.6	39.2	57.1	-																	
5	18.9	3.8	21.3	22.0	-																
6	7.1	10.0	23.6	17.5	22.4	-															
7	22.8	23.1	38.9	39.4	17.2	14.3	-														
8	13.1	13.5	42.9	28.6	34.0	15.2	22.1	-													
9	14.2	18.0	30.0	23.9	22.9	15.7	26.0	37.9	-												
10	20.6	33.4	58.6	53.8	28.6	15.4	33.3	15.2	38.4	-											
11	13.5	10.9	18.4	15.6	42.0	20.0	17.5	31.8	32.3	32.0	-										
12	14.7	17.3	24.4	30.3	25.6	7.3	20.3	22.7	26.1	24.2	15.9	-									
13	17.7	13.3	23.5	23.9	19.0	8.4	17.7	16.7	18.2	22.4	16.7	14.0	-								
14	21.0	26.4	20.8	36.0	45.7	19.4	24.5	35.0	41.7	41.3	40.6	27.4	22.4	-							
15	26.9	45.1	61.4	49.4	21.0	14.4	34.3	33.5	41.9	40.1	35.2	28.1	20.4	42.6	-						
16	20.1	19.7	21.9	33.7	33.7	6.2	23.4	10.1	20.9	18.8	16.7	25.2	11.6	31.7	44.2	-					
17	19.7	9.6	2.5	3.8	5.6	6.6	0.0	7.6	24.8	22.9	12.4	19.9	15.2	25.3	42.0	26.4	-				
18	14.7	33.3	61.6	51.0	20.3	17.7	33.6	37.5	18.1	46.5	14.3	13.1	14.6	26.4	52.3	11.6	6.0	-			
19	17.6	14.0	32.9	33.6	22.7	5.2	26.4	27.5	29.4	31.6	24.2	16.0	13.7	31.4	23.9	14.6	12.1	29.2	-		
20	22.7	48.1	70.0	58.9	20.8	25.4	36.3	40.2	39.5	64.3	23.6	30.5	28.5	38.2	59.9	30.8	34.7	59.4	40.6	-	
21	37.8	49.9	56.1	52.0	48.0	13.7	36.8	25.1	36.9	43.7	37.1	24.2	23.0	46.8	52.5	52.8	49.2	41.0	21.5	60.2	-
ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

Table 6. Password reuse (in percent)

As a result of our analysis we found 68.5 million email addresses that appear in more than one data breach. Within these email addresses, we could find ≈ 19 million email addresses (27%) with maximal cliques, which means they reuse passwords across websites with at least 70% similarity.

To find out the addresses that exactly reuse the same password, we set the minimum clique score to 1.0. In the end, we found about 13.7 million addresses (20%) with this property. Approximately 12.9 million of these addresses use exactly the same password for 2 websites, about 825.000 addresses use the same credentials for 3 websites and about 60.000 addresses use the same login data for 4 different websites.

Source: Jaeger et al. (2016)

HKMA: Cyber Resilience Assessment Framework (C-RAF)

- Step 1: Inherent risk assessment

Image source: https://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20160518e2.pdf

HKMA: Cyber Resilience Assessment Framework (C-RAF)

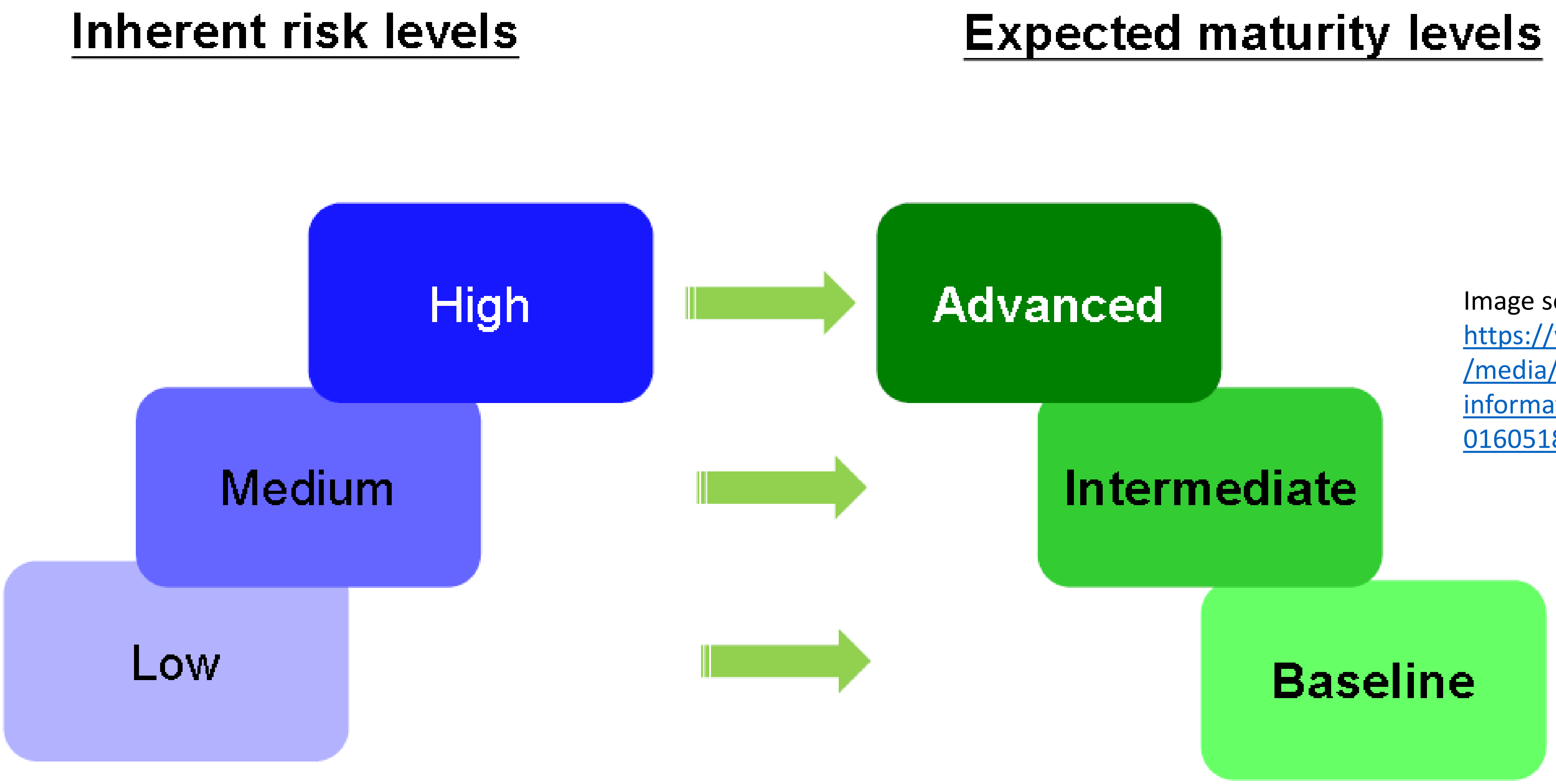
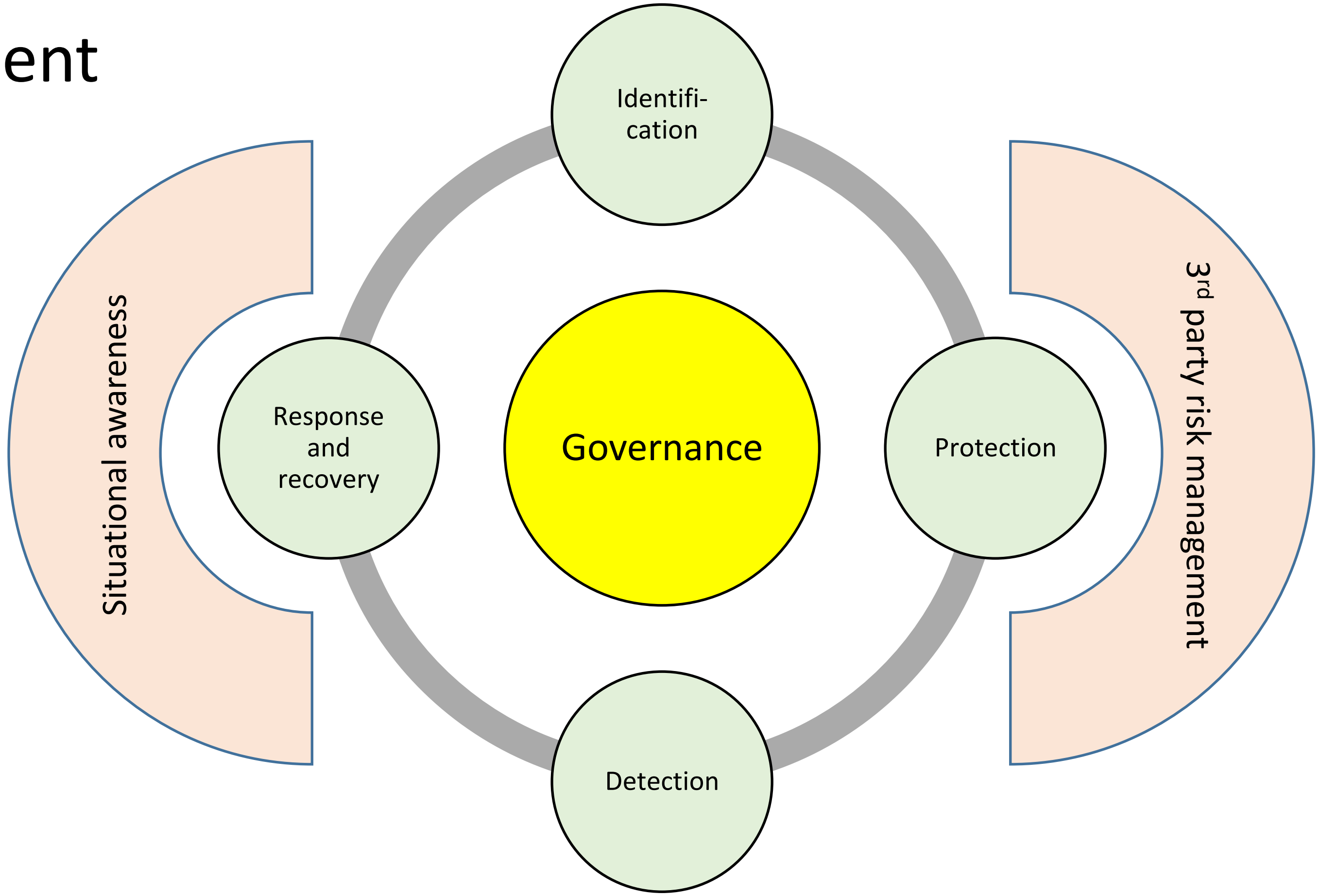


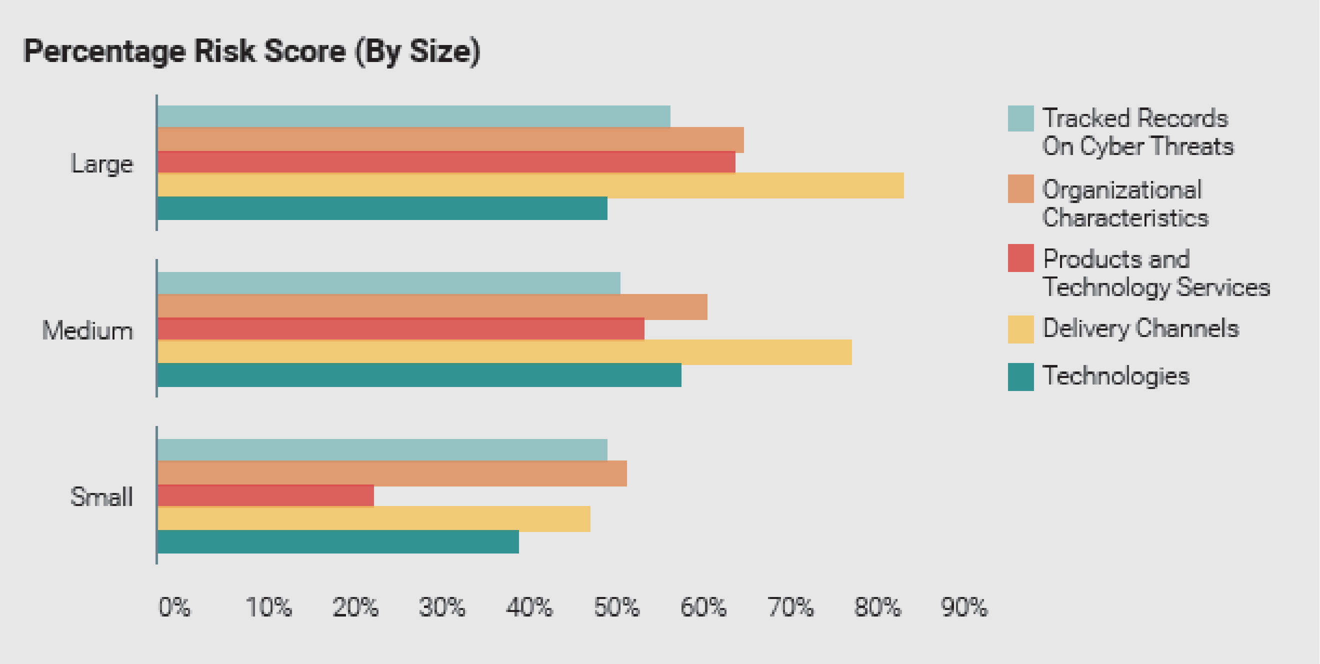
Image source: https://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20160518e2.pdf

HKMA: Cyber Resilience Assessment Framework (C-RAF)

- Step 2: Maturity assessment
  - Seven domains



C-RAF Results



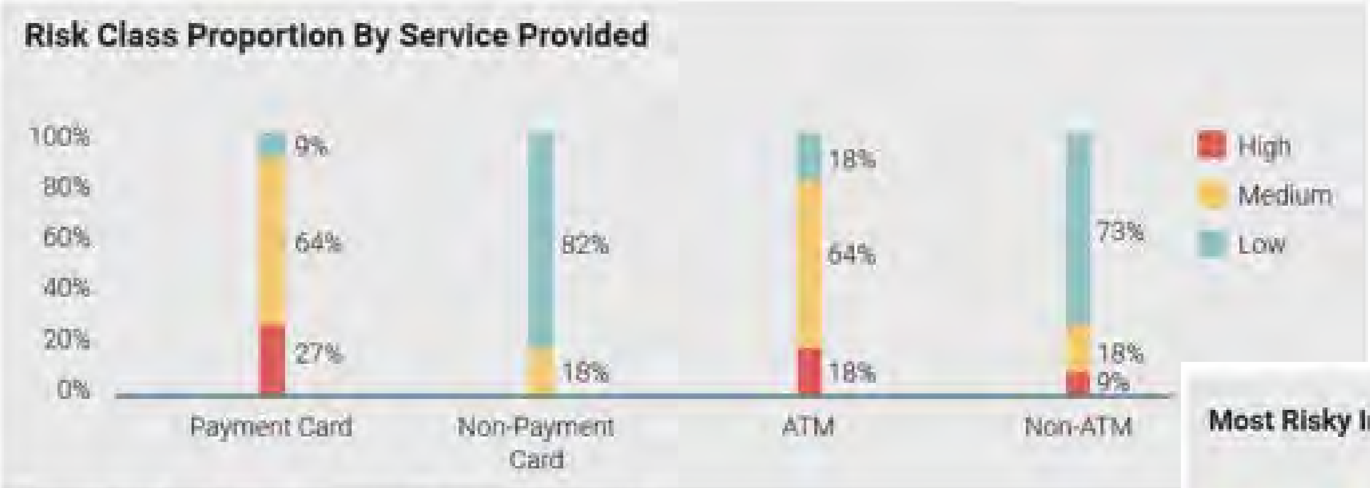
[Exhibit 18] Percentage risk score across the three equity categories

[Exhibit 12] Inherent Risk Assessment – risk score comparison

[Exhibit 15] Relationship between AIs' equity and their overall risk score

First insight: the risk need not come from technology!

C-RAF: Where are the Risks?



[Exhibit 24] Risk class proportion by service provided

[Exhibit 20] Most and least risky indicators by risk score

Are these consistent with what you observe in your company?

C-RAF: Where are the Risks?

Risk sub-domain	Percentage Point Difference: Medium - Low	Percentage Point Difference: High - Low
Network risks	8%	14%
Third-party risks	7%	54%
Internal risks	26%	16%
Internet presence	23%	30%
Mobile presence	56%	67%
Social media presence	16%	23%
ATM	38%	38%
Payment card risks	32%	36%
Fund transfer risks	11%	20%
Client services	28%	5%
Size risks	8%	11%
Service risks	12%	31%
Cybersecurity staffing risks	-5%	20%
Frequency	-3%	9%
Variety	-11%	2%

* in percentage points

- Technologies
- Delivery Channels
- Products and Technology Services
- Organizational Characteristics
- Tracked Records On Cyber Threats

- Top 3 in each column
- Bottom 3 in each column

Risk sub-domain	Percentage Point Difference: Δ ATM & Non-ATM	Percentage Point Difference: Δ Payment & Non-Payment
Network risks	12%	14%
Third-party risks	7%	17%
Internal risks	14%	21%
Internet presence	15%	21%
Mobile presence	45%	58%
Social media presence	15%	21%
ATM	55%	48%
Payment card risks	38%	41%
Fund transfer risks	18%	19%
Client services	17%	17%
Size risks	15%	15%
Service risks	7%	14%
Cybersecurity staffing risks	-8%	-6%
Frequency	0%	2%
Variety	-7%	3%

- Technologies
- Delivery Channels
- Products and Technology Services
- Organizational Characteristics
- Tracked Records On Cyber Threats

- Top 3 in each column
- Bottom 3 in each column

C-RAF: Controls

Prevention

- Many tools and solutions
  - Firewall, intrusion detection systems, threat intelligence systems, SOC, etc.
  - Security awareness, training, and certification
  - Are they effective?

The Key Challenge (1)

- System interdependency
  - When multiple organizations' systems are connected, the threat will propagate from one system to the others, causing collateral damage to all participants using the same service
  - Examples: Target, British Airways, Facebook-Cambridge Analytica, etc.
- Is standard setting and mandatory compliance really helpful?
  - Better basic protection
  - More inter-connection and dependency (e.g., PCI DSS)

The BA Incident


RISKIQ
Sign Up for the Free Edition Blog Contact Us

Inside the Magecart Breach of British Airways: How 22 Lines of Code Claimed 380,000 Victims

September 11, 2018, Yonathan Klijnsma

On September 6th, British Airways announced it had suffered a breach resulting in the theft of customer data. In interviews with the BBC, the company noted that around 380,000 customers could have been affected and that the stolen information included personal and payment information but not passport information.

Source: RiskIQ

"Often, when developers build a mobile app, they make an empty shell and load content from elsewhere. In the case of British Airways, a portion of the app is native but the majority of its functionality loads from web pages from the official British Airways website."

The Key Challenge (2)

- Potential user reaction

Table 1: Countries with Official Evidence on Government-initiated Filters

Country	Filter Type	Effective Date	Reference
Afghanistan	ISP	24 June 2010	OpenNet Initiative [1]
Australia	PC and ISP	20 August 2007	Parliament of Australia [2]
Bahrain	ISP	14 January 2009	Freedom House [3]
China	PC	8 October 2008	OpenNet Initiative [4]
Finland	ISP	1 January 2007	FINLEX [5]
France	ISP	15 March 2011	Breindl and Wright (2013)
Germany	ISP	18 June 2009	Breindl and Wright (2013)
Japan	Mobile ISP	10 December 2007	Freedom House [6]
Turkey	ISP	22 November 2011	Freedom House [7]
United States	PC	21 December 2000	NCSL [8]

[1] https://opennet.net/blog/2010/06/afghanistan-begins-internet-filtering-with-gmail-facebook
[2] http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1415/InternetFiltering
[3] https://freedomhouse.org/report/freedom-net/2011/bahrain
[4] https://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc
[5] http://www.finlex.fi/fi/laki/ajantasa/2006/20061068
[6] https://freedomhouse.org/report/freedom-net/2013/japan
[7] https://freedomhouse.org/report/freedom-net/2012/turkey
[8] http://www.ncsl.org/research/telecommunications-and-information-technology/state-internet-filtering-laws.aspx

Source: Ke et al., working paper

Government Filtering Effect

DV: Compromise rate	(1) Main model	(2) China only	(3) Australia only
Filter scheme	0.182***	0.120*	0.251***
	(0.0556)	(0.0656)	(0.0606)
Number of autonomous systems	-0.117***	-0.122***	-0.122***
	(0.0231)	(0.0195)	(0.0201)
Fixed-line subscription rate	0.00975	0.0107	0.00993
	(0.0113)	(0.0119)	(0.0115)
Internet penetration rate	-0.00645	-0.00666	-0.00663
	(0.00769)	(0.00767)	(0.00775)
Observations	71424	69936	69936
R-squared	0.765	0.768	0.762
# of countries	48	47	47
# of days	1488	1488	1488

Robust standard errors clustered at the country and day levels are in parentheses: *** p<0.01, ** p<0.05, * p<0.1.
Country-fixed effect, day-fixed effect and country-specific linear time trends are included in all models.
The coefficients of fixed effects are not shown for brevity.

Source: Ke et al., working paper

User Reaction to Filtering

(a) Proxy server

	China and Australia			China only			Australia only		
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
IV/DV	GSI	CR	CR	GSI	CR	CR	GSI	CR	CR
Filter schemes	0.204***		0.174***	0.167***		0.114*	0.239***		0.242***
	(0.0318)		(0.0547)	(0.0359)		(0.0651)	(0.0383)		(0.0610)
Google search index		0.0391**	0.0382**		0.0360*	0.0357*		0.0401**	0.0394**
		(0.0188)	(0.0187)		(0.0188)	(0.0188)		(0.0189)	(0.0189)
Observations	71424	71424	71424	69936	69936	69936	69936	69936	69936
R-squared	0.654	0.765	0.765	0.658	0.768	0.768	0.654	0.762	0.762
# of countries	48	48	48	47	47	47	47	47	47

Source: Ke et al., working paper

User Reaction to Filtering

(b) Virtual private network

	China and Australia			China only			Australia only		
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
IV/DV	GSI	CR	CR	GSI	CR	CR	GSI	CR	CR
Filter schemes	0.155		0.180***	0.315***		0.116*	-0.0245		0.251***
	(0.122)		(0.0573)	(0.0538)		(0.0667)	(0.0260)		(0.0605)
Google search index		0.0144	0.0141		0.0142	0.0140		0.0143	0.0143
		(0.0132)	(0.0131)		(0.0131)	(0.0131)		(0.0133)	(0.0132)
Observations	71424	71424	71424	69936	69936	69936	69936	69936	69936
R-squared	0.541	0.765	0.765	0.538	0.768	0.768	0.535	0.762	0.762
# of countries	48	48	48	47	47	47	47	47	47

Source: Ke et al., working paper

User Reaction to Filtering

(c) Tor

	China and Australia			China only			Australia only		
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
IV/DV	GSI	CR	CR	GSI	CR	CR	GSI	CR	CR
Filter schemes	-0.144		0.183***	-0.367***		0.123*	0.0986**		0.250***
	(0.164)		(0.0546)	(0.0435)		(0.0657)	(0.0385)		(0.0607)
Google search index		0.00819	0.00829		0.00841*	0.00851*		0.00930*	0.00926*
		(0.00500)	(0.00498)		(0.00501)	(0.00499)		(0.00482)	(0.00484)
Observations	71424	71424	71424	69936	69936	69936	69936	69936	69936
R-squared	0.514	0.765	0.765	0.515	0.768	0.768	0.515	0.762	0.762
# of countries	48	48	48	47	47	47	47	47	47

Source: Ke et al., working paper

The Key Challenge (3)

HKUST BUSINESS SCHOOL 香港科大商學院 WORLD CLASS IN ASIA

The Economics of Cybersecurity

$$Prob(committing\ cybercrime)$$
$$= f(expected\ net\ benefit)$$
$$= \underline{g(revenue\ from\ crime)} - \underline{h(cost\ of\ crime)}$$

Why did the criminals attack us?

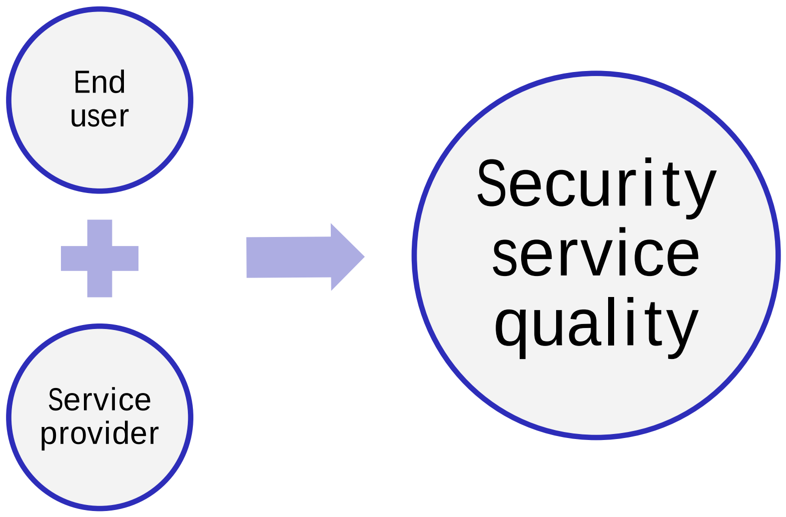
How to increase this?

How to motivate better protection?

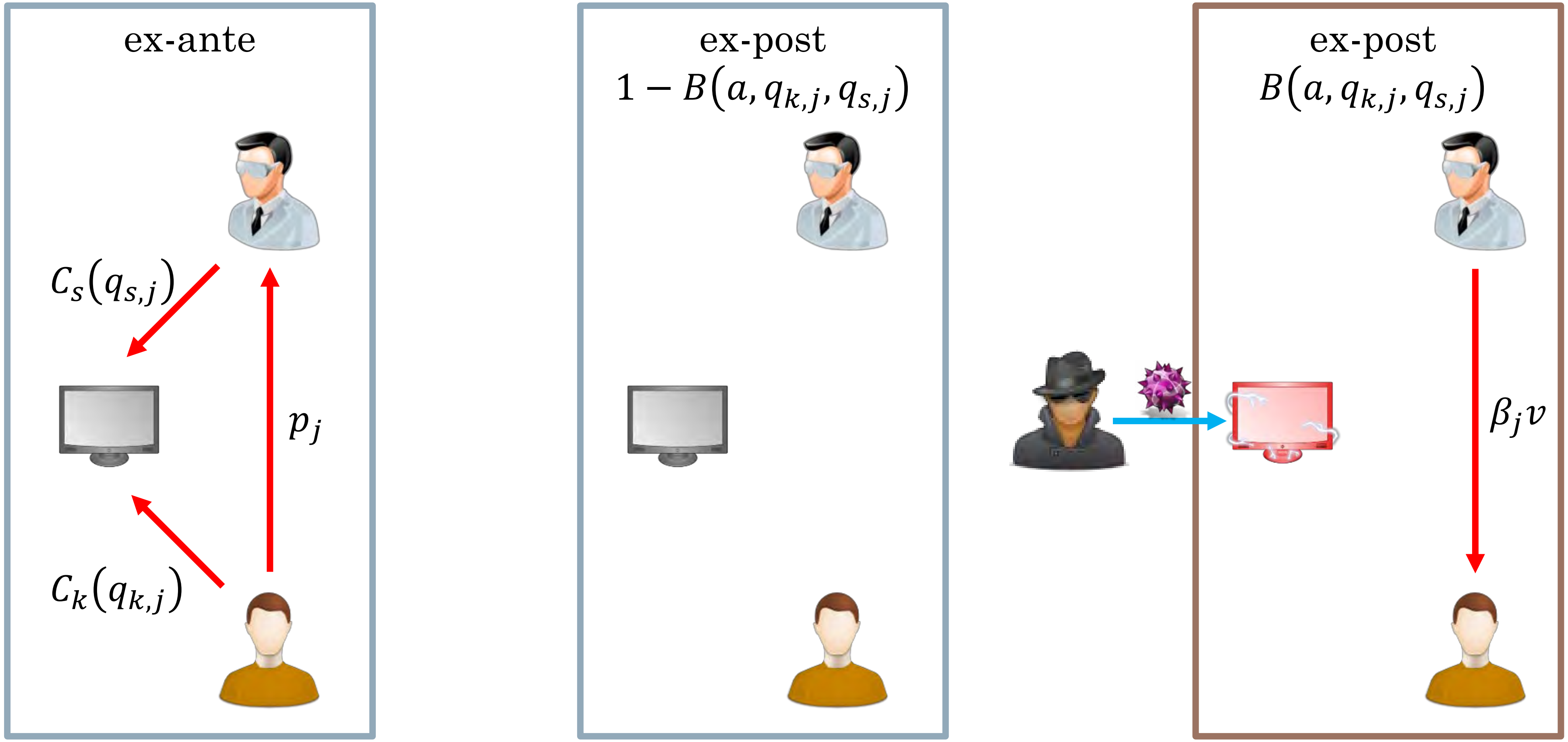
The Economics of Cybersecurity

- Misaligned incentives
  - Quality of security service depends on the effort input by multiple parties – end users, IT staff, service providers, and other related parties
  - This gives rise to the double moral hazard problem
    - Not logging off computer accounts when leaving office
    - Use easily memorable passwords
    - Not responding to firewall alerts

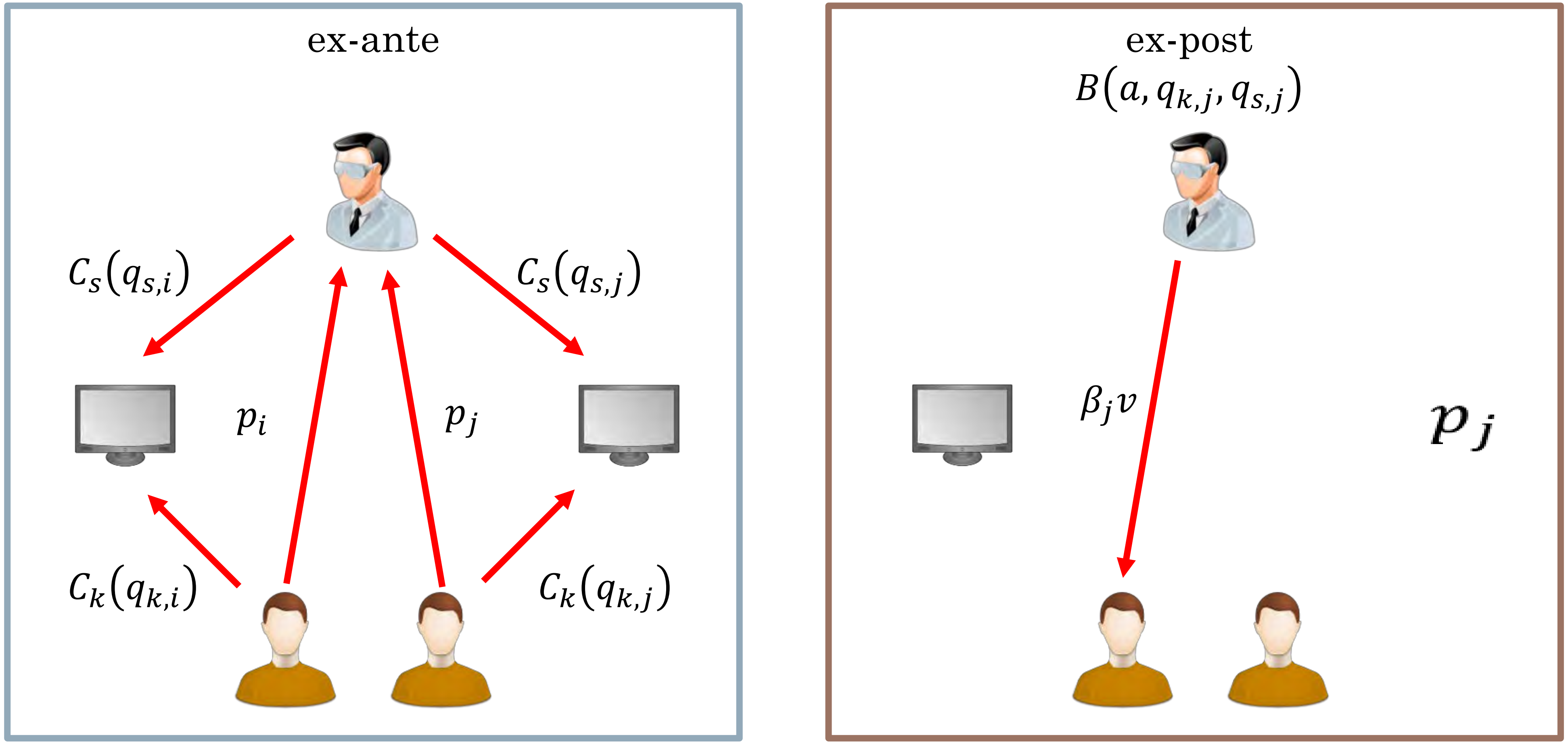
    - Develop sub-standard software
    - Not patching software
    - Not actively monitor IDS and firewall



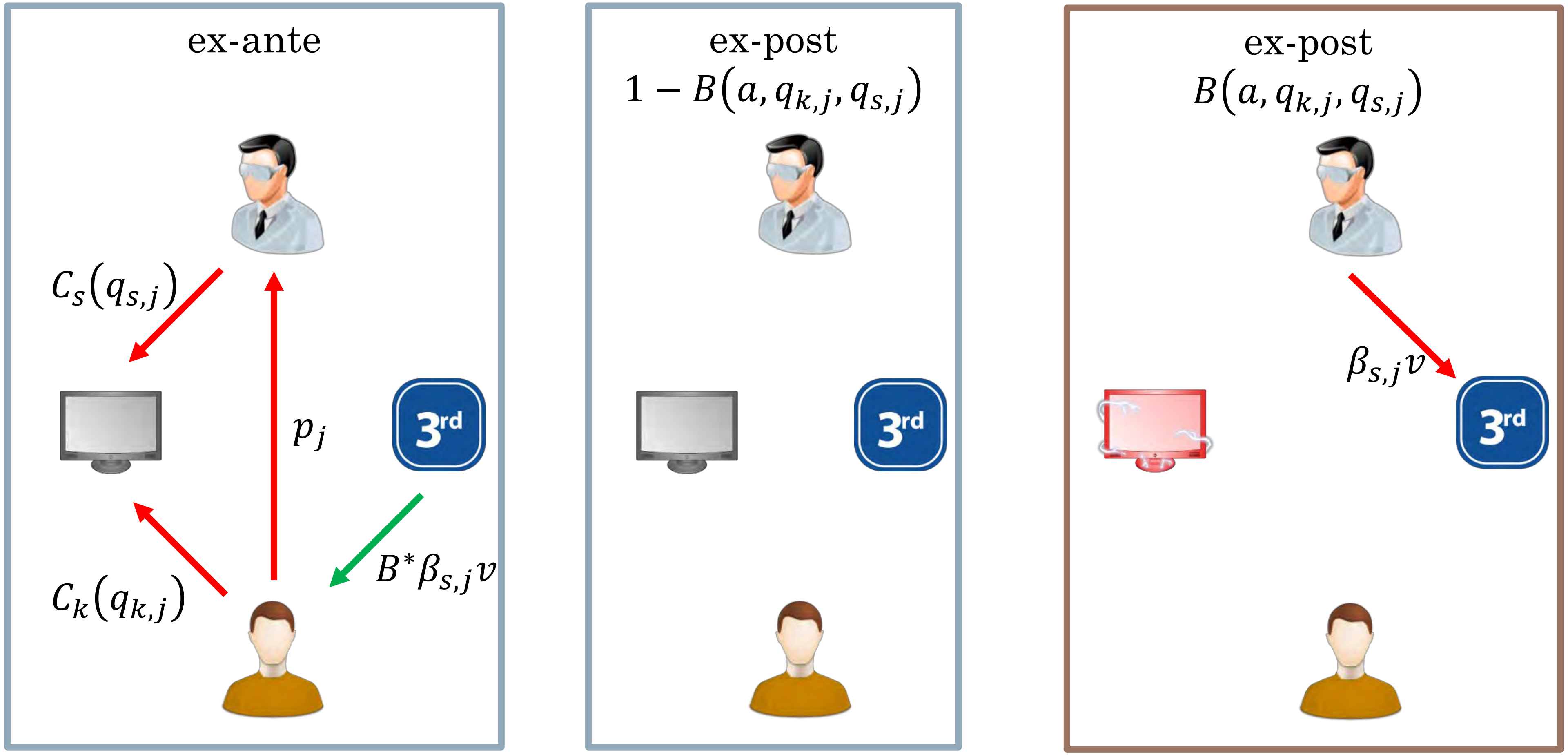
Common Practice: Loss-Based Contract



Theoretical Efficient Solution (1) – Multilateral Contract

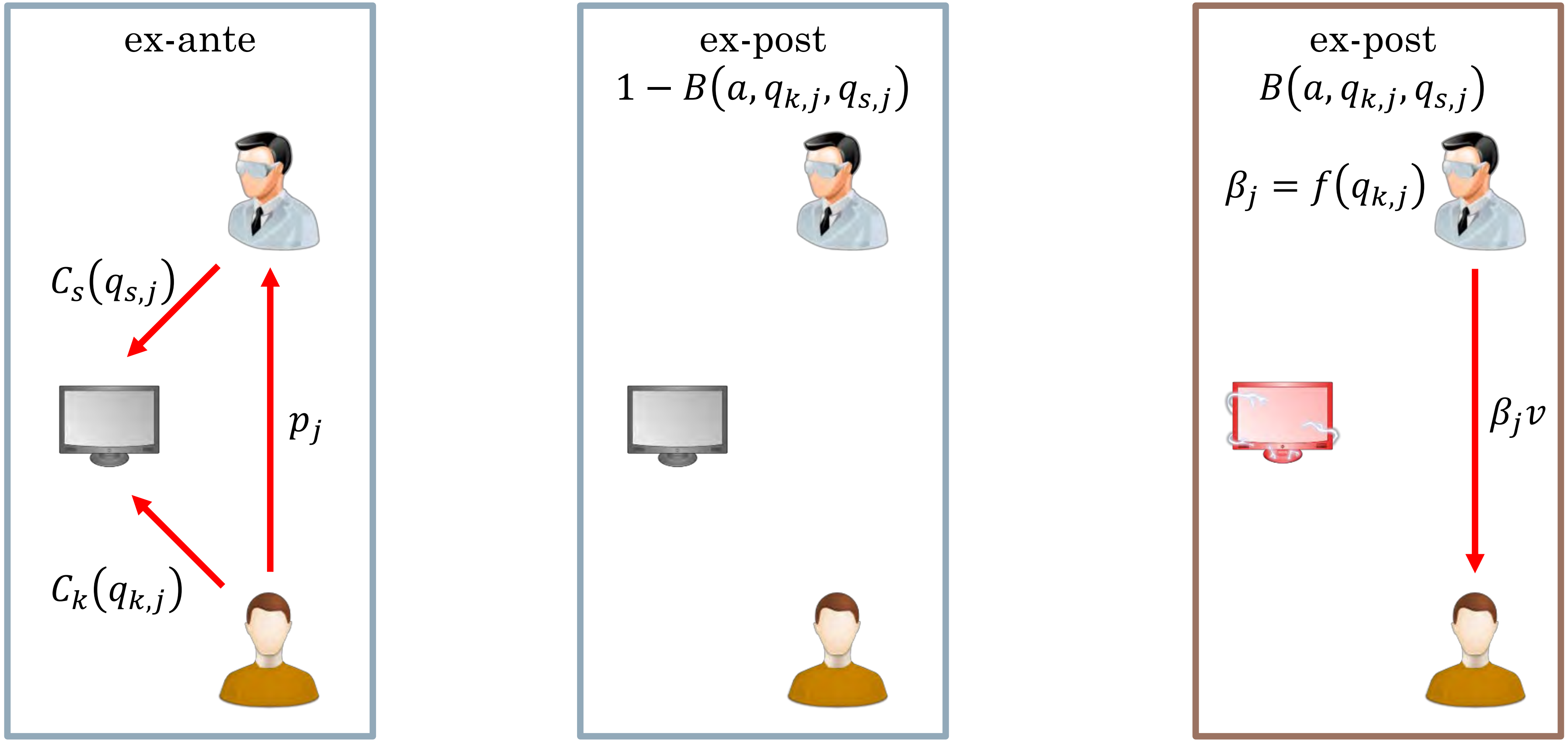


Theoretical Efficient Solution (2) – Reverse Insurance



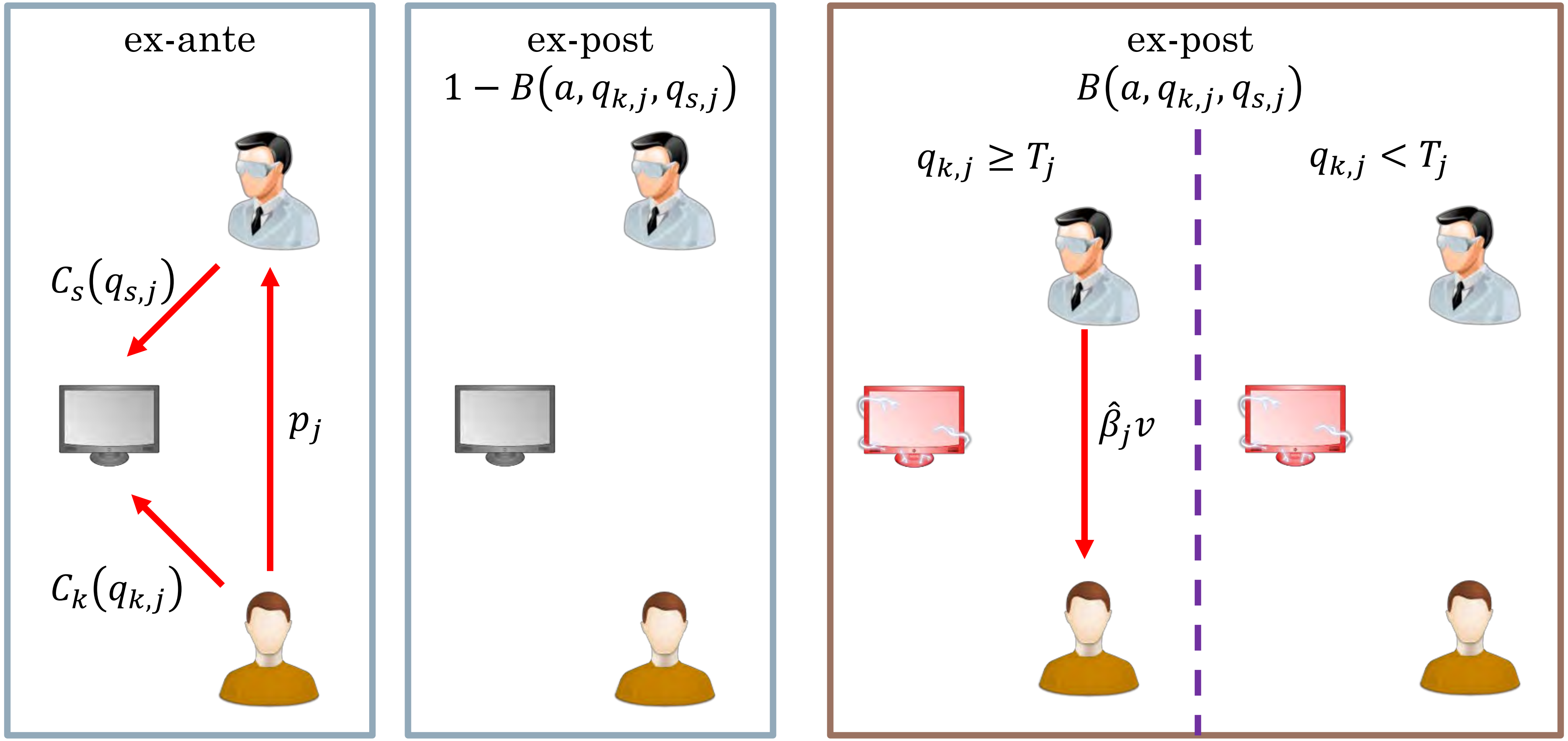
Variable-Liability Contract

(Hui et al. ISR, 2019)



Threshold-Based Liability Contract

(Hui et al. ISR, 2019)



Security Service Contract Design

- Liability needs to be assigned properly to incentivize user protection
  - Typical loss-based liability contracts don't work very well
- With after-event auditing, we can allocate liability to end-users based on actual effort or threshold effort level (Hui et al. ISR, 2019)
  - With limited liability, the threshold-based liability contract produces better protection quality and outcomes than third-party or reverse insurance contracts
  - It is also easier to implement than variable liability contracts and more resilient to auditing errors

Analysis and Conclusions

- Typical cybersecurity solutions are helpful, but they are subject to complementarities
  - Externalities due to system interdependency
  - User response to preventive measures
  - Economic incentives in protecting organizational information systems
- Without addressing these complementary factors, even the best protection tools might not be effective
- Implications on risk management
  - Risk reduction, mitigation, transfer, and termination
  - The focus has always been internal assessment; it's time to go beyond!