



Powering Cybersecurity with Mastercard

September 12, 2023



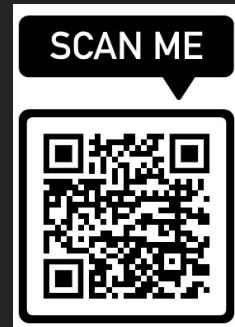
Mandeep Sedha (Mandy)

Mandeep Sedha is a Director of cyber products at Mastercard. She brings 13+ years of experience in cybersecurity, specializing in technology and cyber risk, building enterprise cyber security strategies, Security risk assessments, third party risk assessments, security architecture advisory, c-level presentations. Mandeep has worked in global financial institutions to identify, prioritize and remediate risk.



Deric Karunesudas

Deric Karunesudas is a Director of Cybersecurity Business at Mastercard. He comes with 16+ years of Cyber security experience of specializing in Cloud Security, GRC, Information Risk consulting and Privacy, Security Architecture Assessment, Security analytics and managed Security services business globally. Deric has worked with organizations like Deloitte, RSA, Splunk, NTT and since he has worked in various geographies like APAC, US, Europe and Middle East, he understands various Cyber Security economies & cultures.



We give you 2 Choices !!!



Safeguarding an evolving ecosystem goes beyond protecting transactions



Early Ecosystem



- Well-defined stakeholders
- Protected connections
- Mostly physical acceptance
- Limited large-scale threat
- Growing digital acceptance

Expanding Ecosystem



- New cyber entities
- Increased digital acceptance
- Unprotected connections
- Increased large-scale threat
- More types of transactions

Evolving Ecosystem



- Infinite IoT digital growth
- Countless unprotected connections
- Infinite large-scale threat
- Proliferation of cyber entities
- Increased regulations
- More ways to pay



We are evolving with the ecosystem... from securing transactions to **protecting trust in every interaction**

Continuously monitor and evaluate all points of interaction to identify and address threats and vulnerabilities



Enhance security in the consumer digital transaction journey



Extend security to other types of transactions beyond cards



Expand security beyond transactions to cyber environments



Extend security to mitigate systemic operational risk



Protecting every transaction. Securing every interaction.

Increasing digital data, connections and interactions point to the need for greater security beyond payments



BIGGER DATA

2.5 QUINTILLION

bites of data generated per day by humans and their devices¹



MORE INTERACTIONS

5 BILLION

active internet users around the world year to date (63% of the global population)²

ECOSYSTEM TRENDS



RISE IN ECOMMERCE

\$9 TRILLION

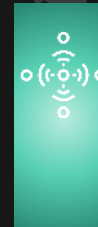
in digital transaction value by 2024 – increasing 60% over 4 years³



INCREASED DIGITAL BANKING

50%

of the world will be using digital wallets by 2024³



GROWTH IN IOT

27 BILLION

is the estimated number of IoT devices by 2025⁴

1. TECHJURY, HOW MUCH DATA IS CREATED EVERYDAY IN 2021? 2021. 2. DATAREPORTAL.COM. 2022. 3. JUNIPER, ONLINE PAYMENT FRAUD 2021-2024. 4. GARTNER, IOT SECURITY PRIMER: CHALLENGES AND EMERGING PRACTICES, 2020.



***“There are only two types of companies:
those that have been hacked,
and those that will be.”***

*Robert Mueller
FBI Director, 2001-2013*





Cybercrime costs the world almost \$7 Trillion, or 4 percent of global GDP¹



1. McAfee in partnership with the Center for Strategic and International Studies (CSIS) - The Economic Impact of Cybercrime—No Slowing Down

2. The Web of Profit: A look at the cybercrime economy - Mike McGuire, University of Surrey

BUSINESS CONTEXT

In a post covid world and with ongoing political crisis, cyber security is an increasing concern across the globe, with the risk of spillover cyberattacks against non-primary targets becoming much more widespread



\$4.2M

average cost of a data breach globally.¹

311%

year-over-year increase in ransomware attacks.²

51%

of companies experience a third-party data breach and do not assess their security and privacy practices.³

90%

Of security leaders believe their organization fall short of addressing cyber risks.⁴

1. Ponemon Institute, 2021 Cost Of A Data Breach Report
2. Forbes 2021, At The Crossroads Of Identity, The Relationship Between Remote Work And Ransomware.
3. Securelink & Ponemon Institute, 2021 A Crisis in Third-party Remote Access Security.
4. Foundry. 2021 Security Priorities Study





Kevin Kelly

@kevin2kelly



When you see the adjective "smart" applied to things, as in smart home, smart clothes, smart toys, smart phone -- substitute the term "hackable." They always come together.



DARK MARKET



'Gripping'
Sunday Times

**HOW HACKERS BECAME THE
NEW MAFIA**

MISHA GLENNY

THE AUTHOR OF
THE SUNDAY TIMES TOP 10 BESTSELLER *MCMAFIA*

Z E R D A Y S

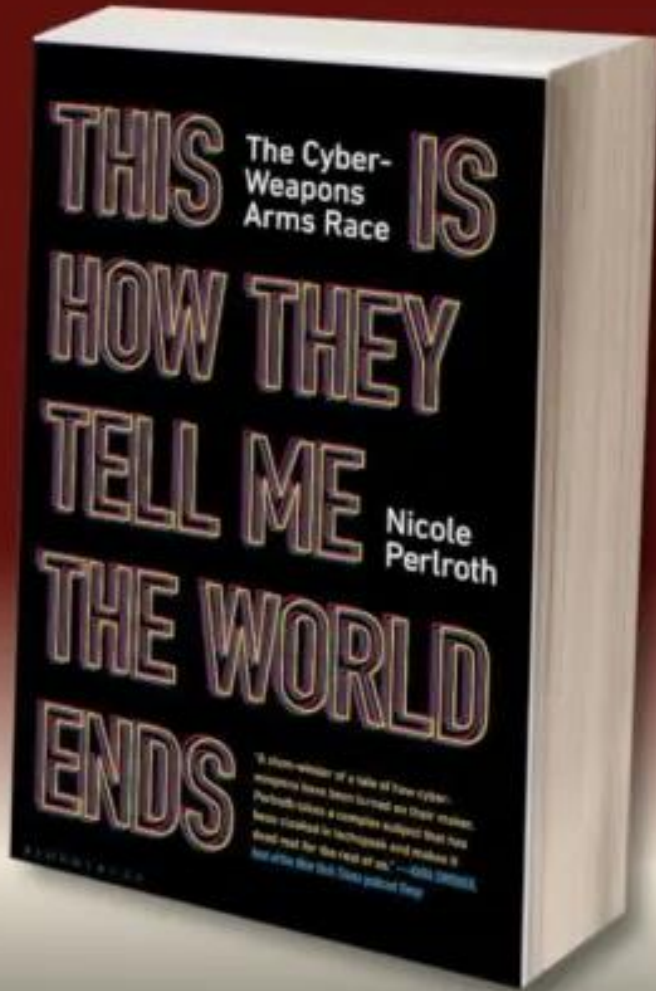


WORLD WAR 3.0

```
start = time.time()
result = func(*args, **kwargs)
print "The function (._name_) took {:.15f} seconds
return result
return wrapper

@limit
def solve_password(word):
    global attempted_password
    for character in word:
        for entry in list_of_c
            if character == en
```





Zero Day Market



CAN'T GET HACKED

**IF YOU DON'T GIVE ANYONE
A COMPUTER**

Make

Opening
Mon
Tue-Thu
Fri-Sat
Sunday

Top factors driving cyber trends in Thailand

Beyond rapid digitalization and growing interconnectivity, cyber trends in Thailand are shaped by the following three key factors:



Social Economic



- For the duration of the observed period, financial motivation was the most prominent driver of cybercrime .
- The economic downturn can be exacerbated by the pandemic. Databases exposed to the internet have grown steadily throughout the year with increase in digitalization ¹.
- Rapid digitalization – both in public and private sectors – on digitalization led to the advent and growth of new payment methods amid a spike in fraud, scams and tech enabled financial crimes.

Political



- Escalation in politically driven cyber activities is a known pattern, especially when notable political events take place. This can be caused by internal conflict and/or global distress such as wars.
- State sponsored hackers allegedly targeted Southeast Asia's government, military offices.

Regulatory



- The cybersecurity maturity of the businesses is typically shaped by the laws and regulations of the country.
- The current cybersecurity regulatory structure is largely decentralized, and this leads to inefficiencies in quickly mitigating and securing against cyber risks
- As the National Cybersecurity Agency (NCSA) of Thailand ramps up new security requirements and regulations quickly, organizations will need to allocate more resources and in an efficient way to navigate compliance challenges.¹⁶ This in turn drive and direct organizational behavior towards adopting a more robust cybersecurity infrastructure.

Sources: Cyber insights report, Mastercard

What should organizations do?

Both public and private organizations must work closely to navigate newly enacted cybersecurity laws and regulations. Without clear alignment in expectations, organizations will likely spend additional resources to figure out the intent and desired outcome of enacting these laws and regulations.

Organizations must be aware of factors that shape their threat landscape. This can be achieved by continuously monitoring popular threat actors and attack methods globally, in their region and the industry. Based on the threat landscape, the current cybersecurity control maturity must be assessed and mapped to related threats.

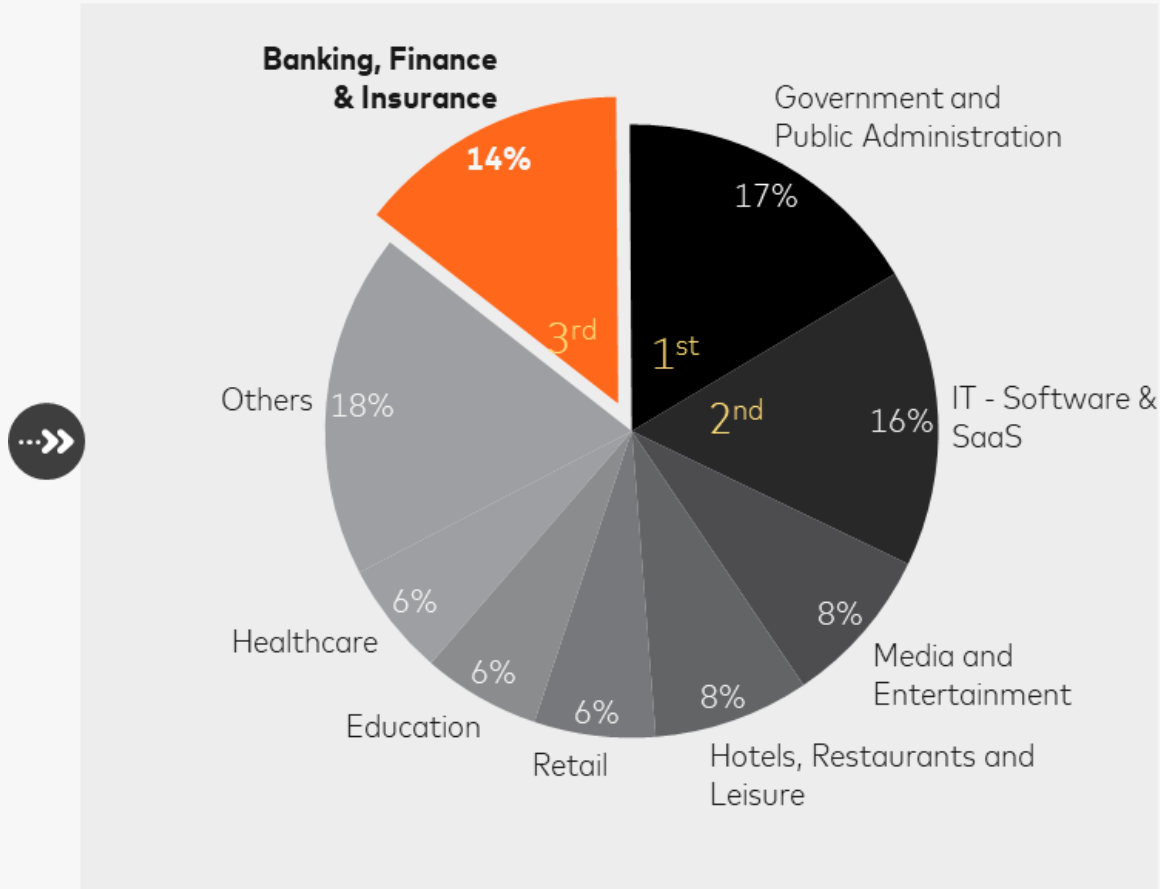
Once initial assessments are complete, the organization needs to design its desired state based on its current capabilities, available resources, business priorities and the severity of the risks.

Finally, a prioritized remediation or maturity roadmap based on a risk and return on investment calculation should be established.

In any case, organizations should identify their most sensitive information and valuable assets to be protected. Protection efforts should be prioritized and optimized by focusing on low hanging initiatives that can yield the best outcomes given the available resources.



Cyber Occurrences by Industries in Thailand



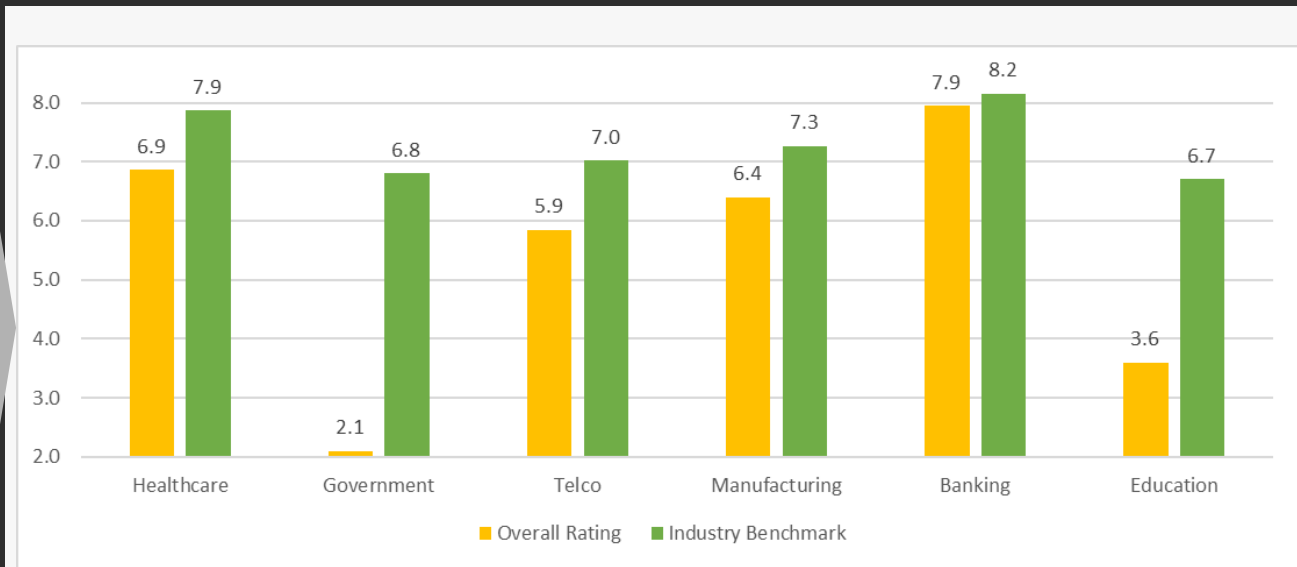
Thailand external assessment

What do RiskRecon ratings indicate?

- RiskRecon ratings include overall rating and at a security domain level
- Ratings are on a scale of 1-10 , lower ratings correlate to higher breach event frequencies
- Prioritized risk ratings for remediation management

Key Observations from Thailand industry-wide Benchmark study:

- All sectors – Healthcare, Government, Telco, Manufacturing, Banking & Educations are benchmarked lower than global peers.
- Government and Education sectors are significantly lower rated as compared to their global peers.



Source: RiskRecon industry benchmark report of select Thailand Industries and Companies



Observations of the attack methods used across attack campaigns targeting BFSI

Email Social Engineering



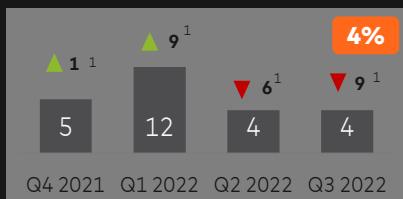
Ransomware**



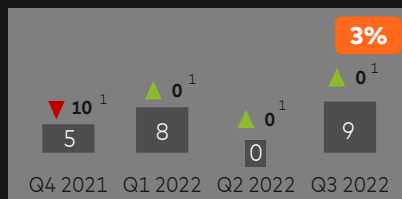
Malware**



Denial of Service



Spoofing/MitM



** Ransomware is Malware in the conventional sense. Recently Ransomware has become so prominent, we have categorized it separate from Malware.

Key Insights

- Malware, Ransomware, and Email Social Engineering attacks were used in around 80% of total attacks in this period.
- Email social engineering was the most common attack vector used by **financially motivated organized crime groups through weaponizing well-known exploits** to propagate itself into networks and devices. This type of attack increased by more than 100% compared to last year.
- Additionally, threat actors are increasingly changing their tactics by first using email social engineering to implement malware on networks using malicious URLs. The use of malicious websites that simulate the login page of corporate sites allows attackers to steal credentials (**credential harvesting**), which are then offered for sale in underground markets; it is driving the trend of "**Access as a service**" in the commercialization of these credentials.
- Significant increase in SMS spoofing has been observed in the Singapore region. Blacklist-based strategy and SMS Sender ID Protection Registry (SSIR) were developed to tackle these issues.

Top assets targeted by threat actors



**Clients Financial
Information**



**Clients Personal
Information**



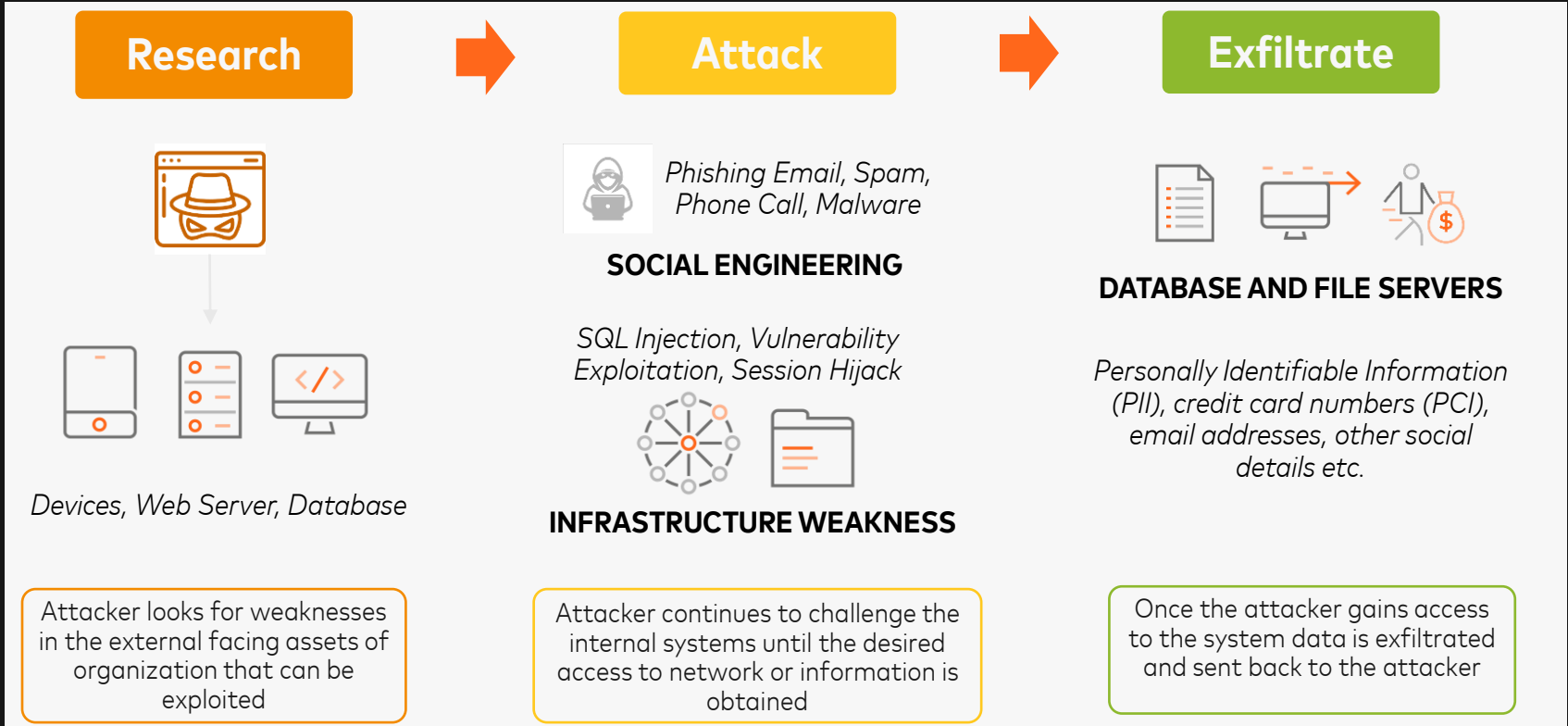
Payment card data



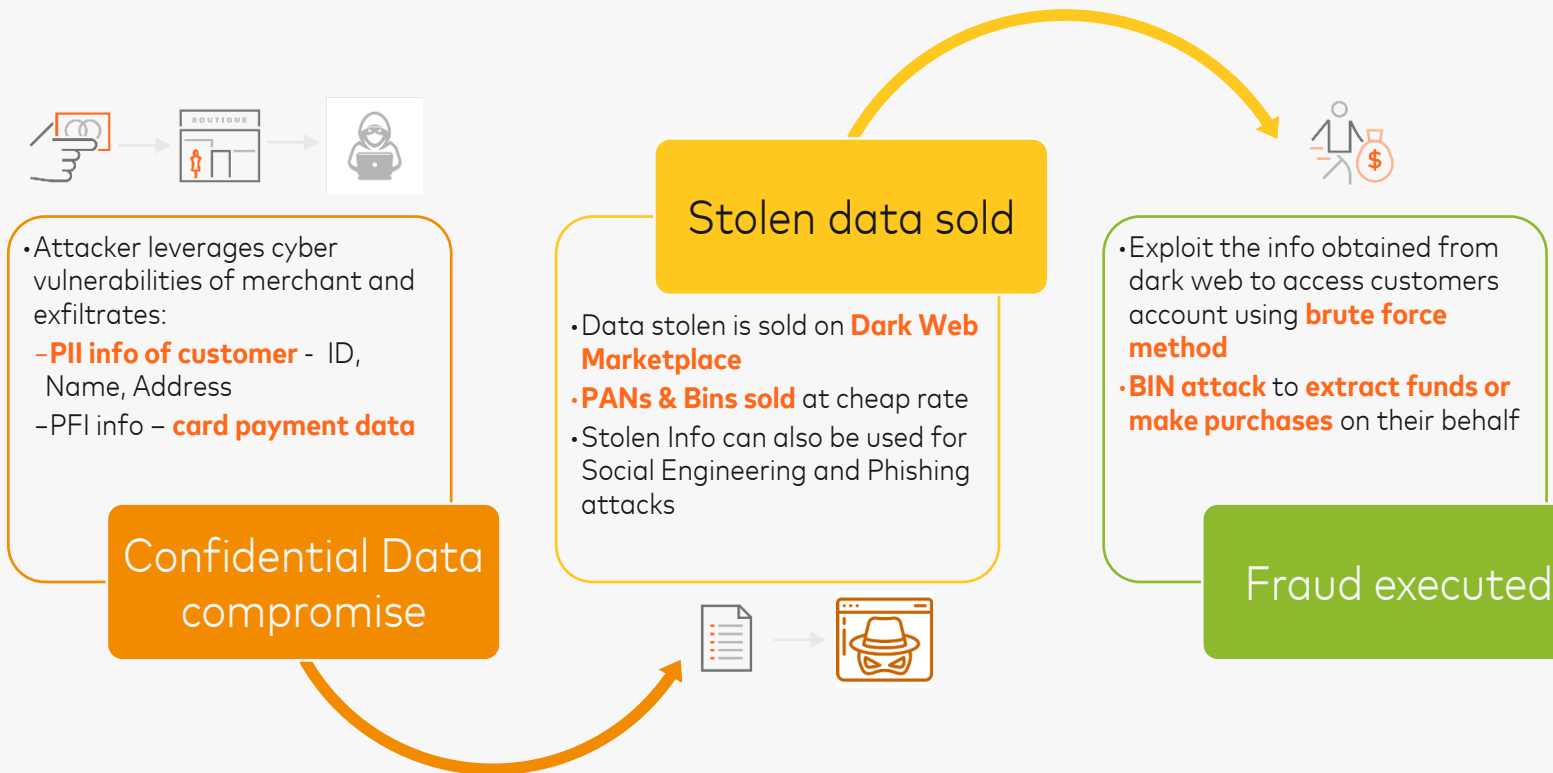
**Available services to
clients**



How Data Breaches Occur



And leads to a fraud attack





THE ADVENTURES OF CISO ED & CO.®

HERE ARE THE CYBERSECURITY TOOLS WE HAVE DEPLOYED - SITM, BASG, HTUS, GTE, AJD, AZS, JEHR, PO2ND, JEJ98SN, SNHD, TRP, MSRP, ...



SO ARE WE SECURE YET?



Our Mastercard offerings help organizations address key cybersecurity concerns



Cybersecurity Risk Quantification

How mature are my cybersecurity controls compared to their importance and what is the financial risk impact of possible cyber security incidents and risk mitigating investments.



Cybersecurity Attack Simulation

How resilient is my technical infrastructure against thousands of real-world cybersecurity attack methods and how can I close the gaps.



Third Party Risk Monitoring

How can I ensure that my third-party providers such as vendors and suppliers adhere to my security requirements and do not risk my assets and how secure is my own external posture.



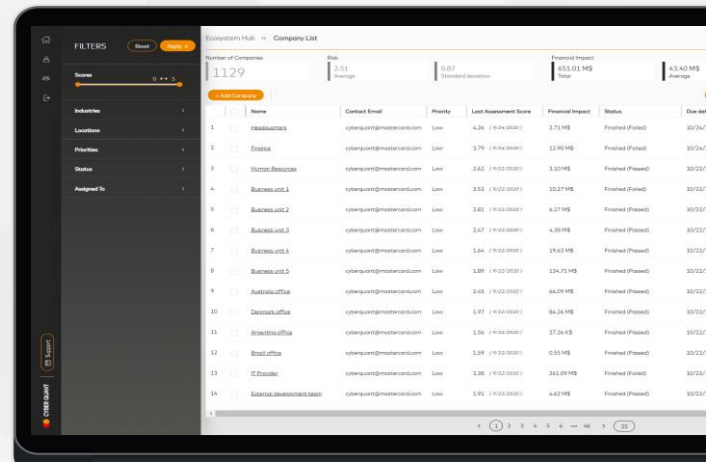
Cyber Strategy & Transformation

Massive cybersecurity breaches have become almost commonplace. Do I have the right strategy, governance and technology to protect my business from emerging cybersecurity risks.



Without proper risk evaluation and quantification, it is **harder** to identify gaps in cybersecurity

With Cyber Quant, organisations can evaluate their risk and financial exposure, based on their defensive capabilities and threat landscape, and prioritise remediation gaps to fit reduce cyber risks.



Name	Contact Email	Priority	Last Assessment Score	Financial Impact	Status	Due Date
1	cyberquant@mastercard.com	Low	4.26 (4/4/2022)	3.71 MS	Finished (Pass)	10/24/22
2	cyberquant@mastercard.com	Low	3.79 (4/4/2022)	12.90 MS	Finished (Pass)	10/24/22
3	cyberquant@mastercard.com	Low	2.82 (4/12/2022)	3.00 MS	Finished (Pass)	10/22/22
4	cyberquant@mastercard.com	Low	3.52 (4/12/2022)	10.27 MS	Finished (Pass)	10/22/22
5	cyberquant@mastercard.com	Low	2.82 (4/12/2022)	4.27 MS	Finished (Pass)	10/22/22
6	cyberquant@mastercard.com	Low	2.47 (4/12/2022)	4.38 MS	Finished (Pass)	10/22/22
7	cyberquant@mastercard.com	Low	1.84 (4/12/2022)	19.63 MS	Finished (Pass)	10/22/22
8	cyberquant@mastercard.com	Low	1.89 (4/12/2022)	124.75 MS	Finished (Pass)	10/22/22
9	cyberquant@mastercard.com	Low	2.42 (4/12/2022)	66.09 MS	Finished (Pass)	10/22/22
10	cyberquant@mastercard.com	Low	1.97 (4/12/2022)	16.24 MS	Finished (Pass)	10/22/22
11	cyberquant@mastercard.com	Low	1.56 (4/12/2022)	27.24 MS	Finished (Pass)	10/22/22
12	cyberquant@mastercard.com	Low	1.59 (4/12/2022)	0.55 MS	Finished (Pass)	10/22/22
13	cyberquant@mastercard.com	Low	2.28 (4/12/2022)	342.09 MS	Finished (Pass)	10/22/22
14	cyberquant@mastercard.com	Low	1.91 (4/12/2022)	4.63 MS	Finished (Pass)	10/22/22

Mastercard in Forrester Wave

2023 (CRQ)



Cyber Quant assesses cyber risk, translates it into financial impact and provides actionable recommendations on risk mitigation

Input

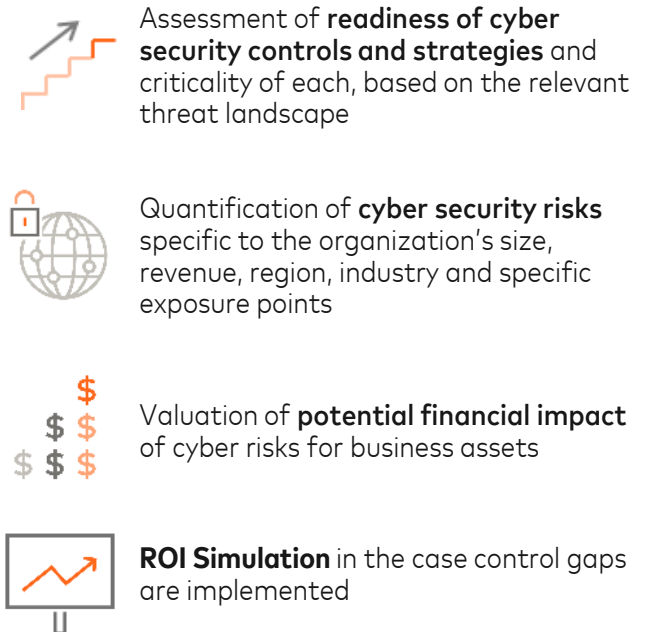


Processing

Organization demographics and characteristics



Output



HOW IT WORKS

- Comprehensive assessment of broad cybersecurity capabilities and risks to assess adherence to security policies, procedures and technical capabilities
- Contextualised analysis of cybersecurity controls and strategies matched to threat landscape
- Strategies to reduce financial costs associated with a breach
- Prioritised risk reduction areas to drive maximum return on investment
- Simulation engine for ongoing evaluation of cyber projects
- Continual updates of cyber practices and projects to account based on changing cyber threats

BENEFITS

CEO & Board

- Organisation-wide risk and financial impact oversight
- Risk mitigation and transference
- Strategic decision support tool

CRO

- Risk Management Review
- Financial impact analysis across business assets and lines
- Cyber Insurance

Compliance Officer

- Compliance Review
- Assessment preparation
- New Regulation preparation

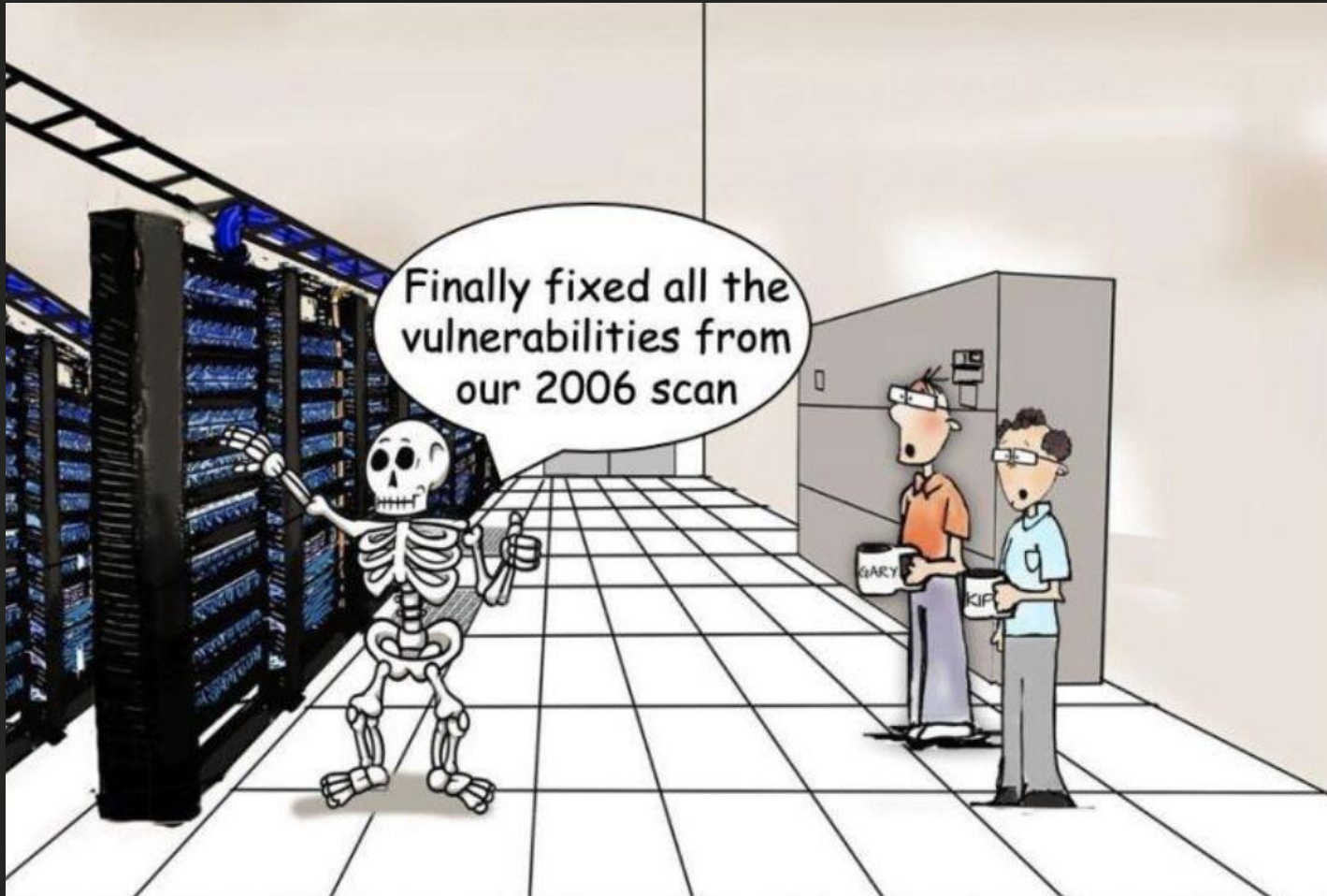
CISO

- Assess the current cyber maturity
- Justify the budget / investment
- Security roadmap and strategy formulation

CFO

- M&A Activity
- Budget prioritisation
- Business Expansion / Contraction





There is no safety without truly understanding today's attackers

Reactive security is no longer enough in cybersecurity. The complexity of today's threats, together with the vast resources and skills of cybercriminals, mean that proactive security is the only way to defend one's cyber turf.

Businesses must now have deep and continuous visibility into the state of their security environments and any vulnerabilities that exist, from the point of view of cybercriminals.



CYBER FRONT

What if the organizations can actively simulate real world cyber threats to validate the effectiveness of their security controls?

What does it do?

Validates that your security infrastructure, configuration settings and prevention technologies are operating as intended. Understand how effective the active protection capabilities are being utilized.

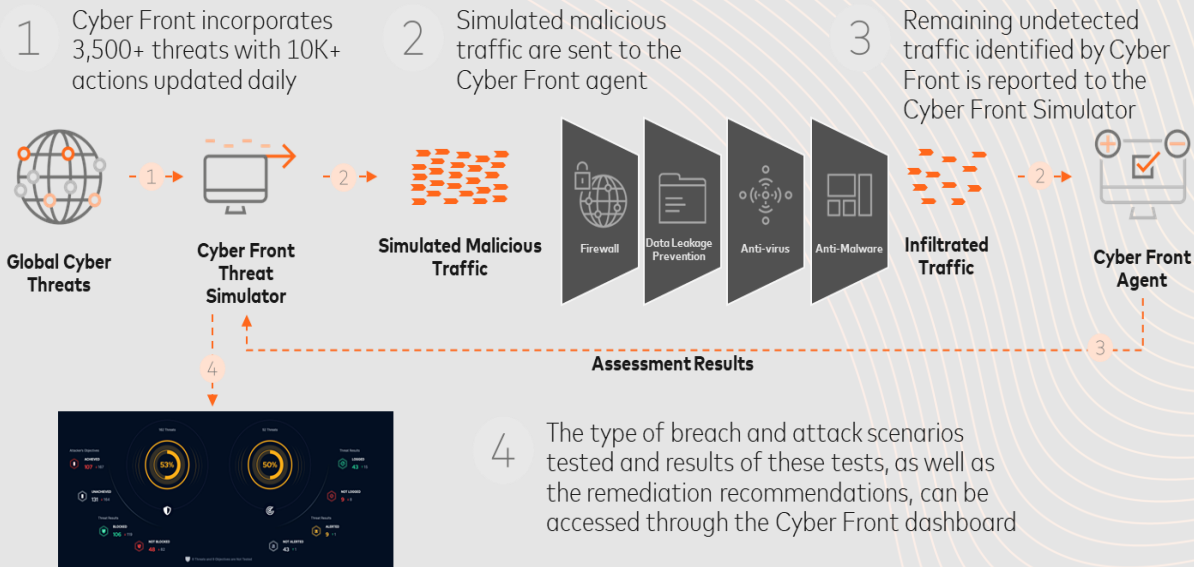
Grants your organization the ability to continuously test existing security infrastructure, without the need to wait for vulnerability scanning windows. It allows your organization to focus on threats and attack vectors, helping your organization understand the probability of threats materializing.

Validate detect and respond capabilities as part of a cyber response exercise where security operations staff and incident responders are evaluated if they can detect specific attacks and respond accordingly.

*Cyber Quant solution is fitting for use cases for small, medium, and large enterprises. It is also available for market-wide initiatives. It can be one-time or subscription service.

How it Works:

Cyber Front is an intelligence-driven continuous security validation platform that simplifies security operations and optimizes defenses by simulating cyber threats without affecting the production systems.



With Cyber Front, your organization can actively validate effectiveness of your existing cyber security protection mechanisms, understand your detection capabilities and improve their response processes.



BENEFITS

By improving detection and responding to current threats, organisations can improve and optimise their cyber resiliency.

1



Lower Risk

10% reduction in breach risks by identifying misconfigurations with historical and real-time visibility for cyber-threat readiness, and to fix potential defence gaps before a compromise*

2



Lower Capital Expenses

7% improvement in efficiency using existing cybersecurity infrastructure and continual testing capabilities with lower dependency on penetration testing services*

3



Lower Operational Expenses

Save on analysis and response times, with focus on exploitable misconfigurations, resulting in better use of limited resources

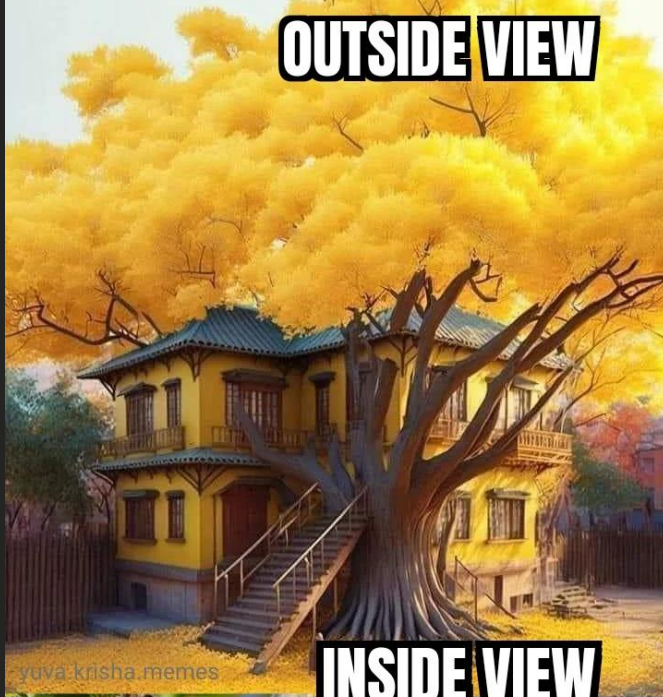


Answer three key questions:

1. Did preventative and detective controls work as anticipated?
2. Does the security operations center (SOC) have the capabilities and processes to respond to detected alerts?
3. How should the organisation address exploits that were neither prevented nor detected?

* Ponemon Institute, 2020 Cost of a Data Breach Study (US\$)

OUTSIDE VIEW

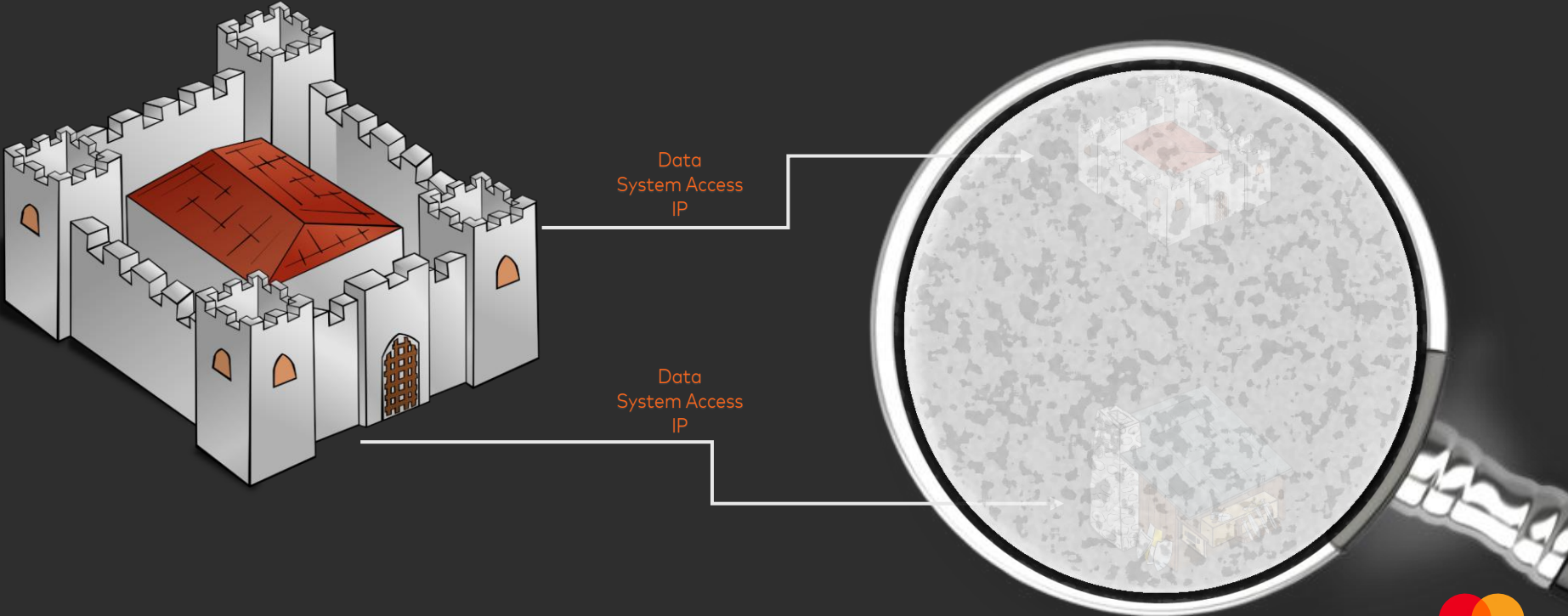


yuva.krisha.memes

INSIDE VIEW



Why We Do Third-Party Risk Assessments?



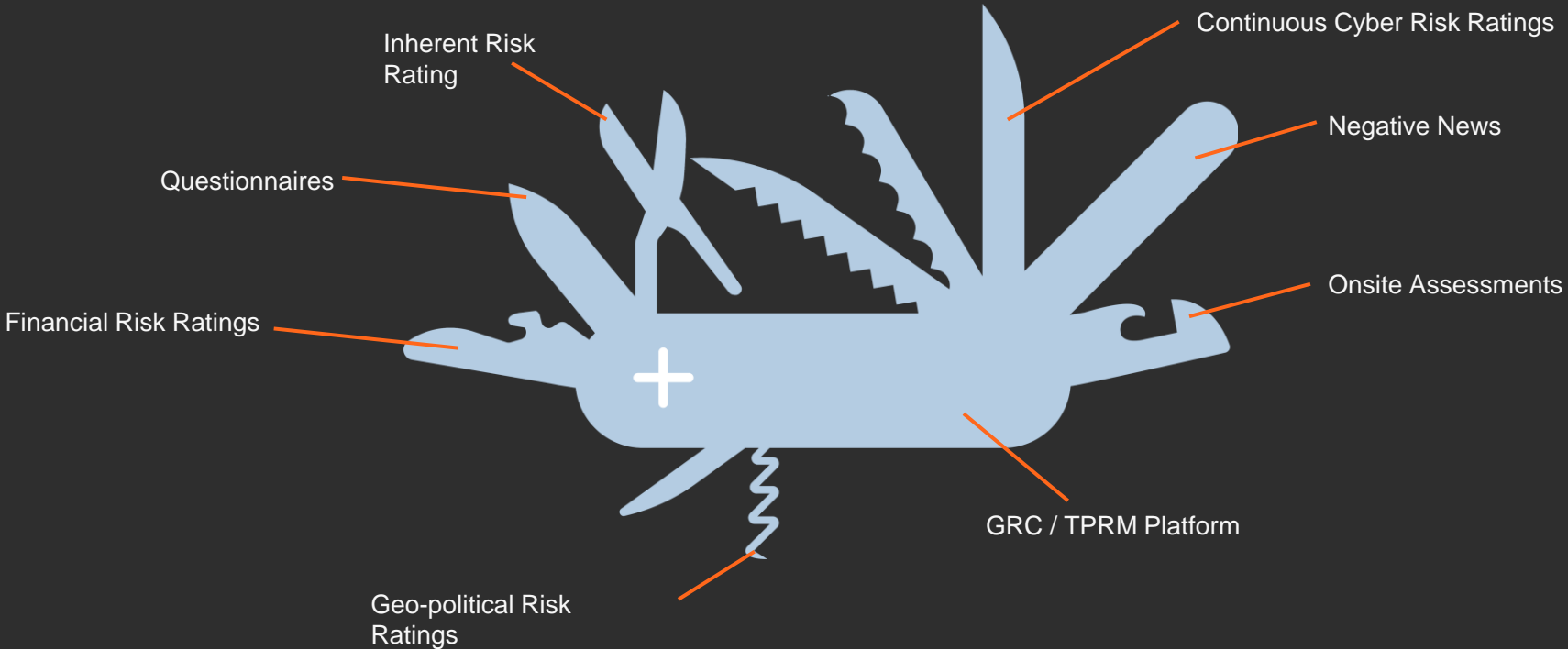
What Many Third-Party Programs Likely Focus On



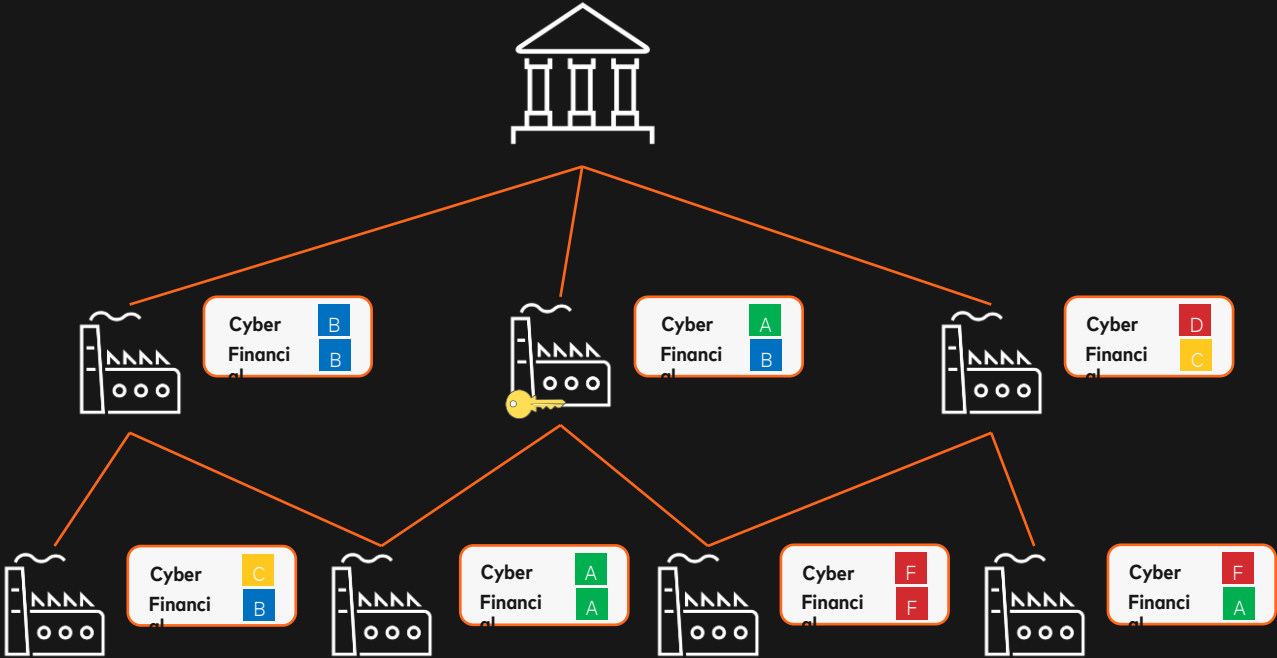
What Your Extended Supply Chain Really Looks Like



Designing a TPRM Program for Situational Awareness



Utilizing Situational Awareness – Who is the Weak Link?



What the Data Tells Us About Company X



- 40x more likely to experience a Ransomware event¹
- 4x more likely to experience a breach²
- Lower financial health indicates that they may not recover from either event
- Single point of failure for multiple third-party vendors/suppliers
- Relied on by key vendor/supplier – Potential problem area to address ASAP

1- Predicting Ransomware Event Frequency with RiskRecon Cybersecurity Ratings and Insights, <https://www.riskrecon.com/ransomware-event-frequency-report>

2- Predicting Third-Party Breach Event Frequency with RiskRecon Cybersecurity Ratings, <https://www.riskrecon.com/predicting-breach-frequency>



Understanding and monitoring your organization's own cyber hygiene as well as third parties you do business with

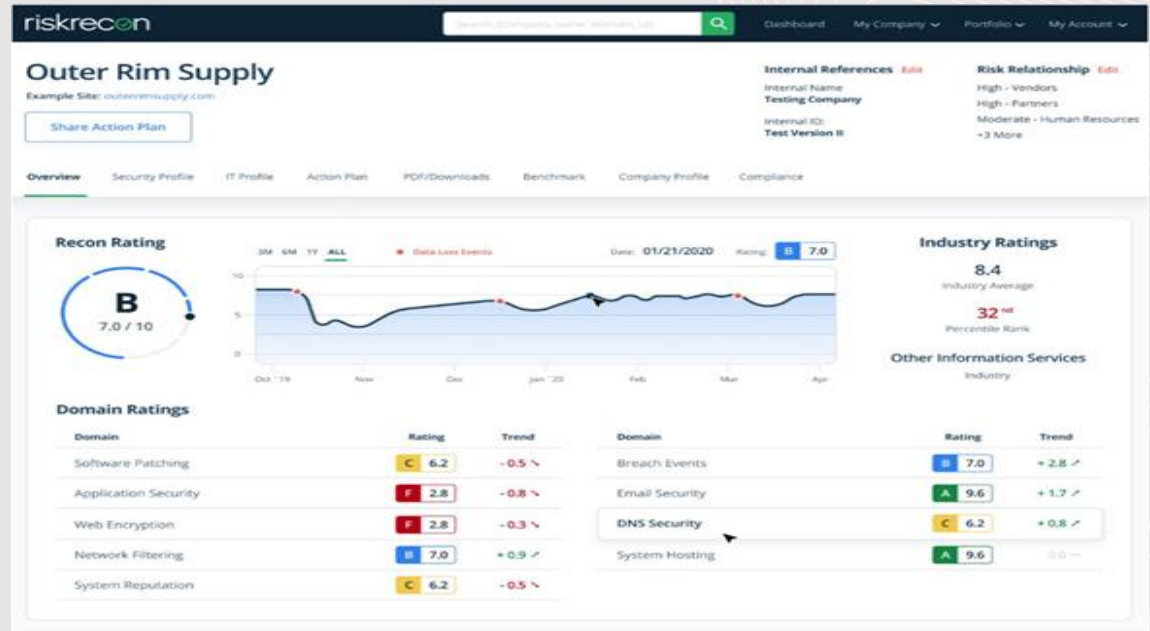
What does it do?

RiskRecon effectively assesses cyber risk from third-party business relationships and proactively monitors the cyber environment of any entity with an online presence to identify cyber risks and vulnerabilities before they can be exploited.

By effectively assessing cyber risk from third parties, organizations can ensure they do not fall victim to cyber attacks from the risks incurred through their business relationships.

How it Works:

RiskRecon leverages supervised machine learning models trained by analysts to efficiently mine the internet for company systems and to ensure accurate company asset attribution as companies shift over time. Thereafter, RiskRecon builds a detailed profile of every asset discovered which includes various security domains and benchmarks them with overall current performance, trends, and industry.



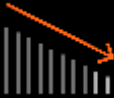
DID YOU KNOW?

RiskRecon asset discovery is engineered to be extraordinarily thorough while having an extremely low false-positive rate of less than 1%.

*Cyber Quant solution is fitting for use cases for small, medium, and large enterprises. It is also available for market-wide initiatives. It can be one-time or subscription service.



Accurate and reliable cyber risk assessments help you reduce losses while saving time and resources



Reduce financial losses from third-party cyber risk

Advanced third-party assessments at an affordable price ensure your cyber environment is not in danger of compromise



Gain greater control and flexibility managing third-party cyber risk

Cyber risk assessments can be performed as often as needed on as many third and fourth-party service providers as needed



Save time and resources managing third-party cyber risk

Automated third-party risk assessments reduce the time taken and the number of manual resources needed to monitor third-party cyber risk



Obtain more reliable, accurate assessments of third-party cyber risk

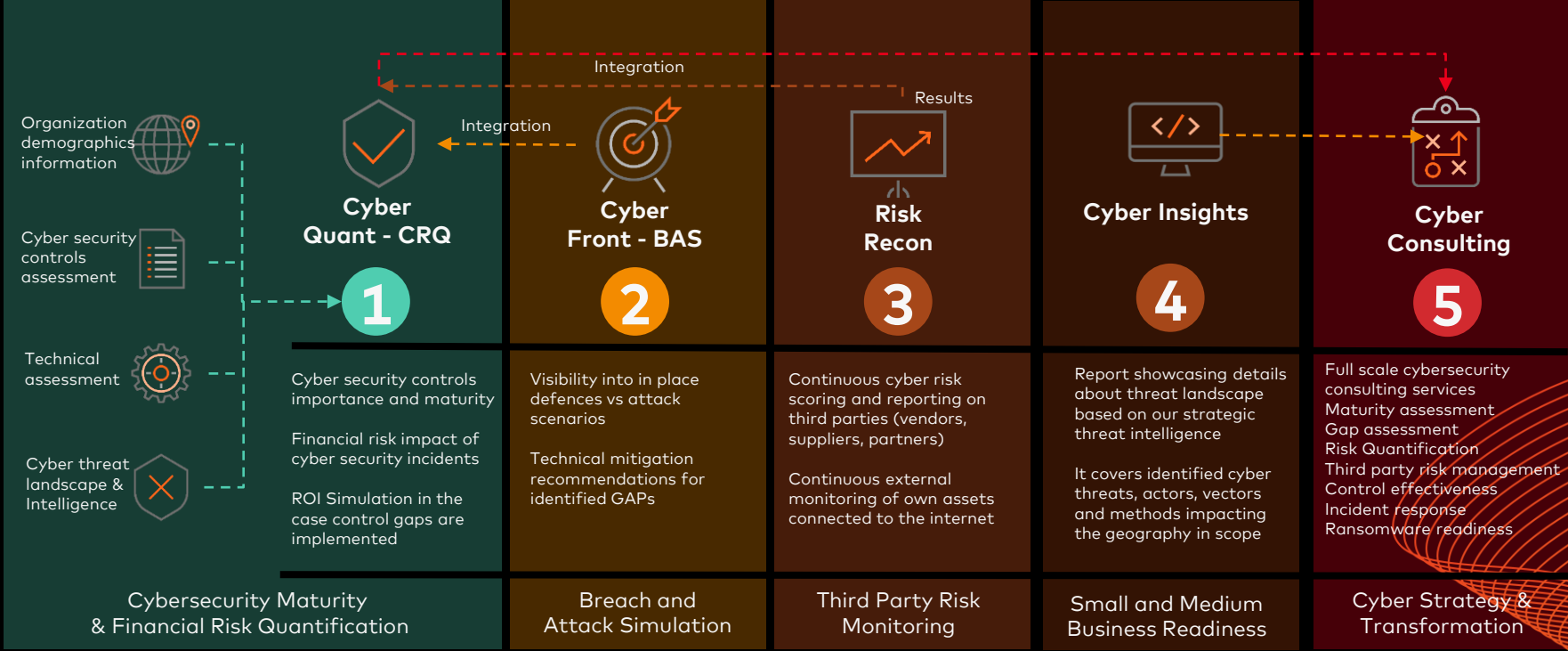
Accurate and verifiable data of third parties collected from public domains ensures cyber risk assessments are completely reliable



Realize a new line of revenue

Additional revenues from offering My Cyber Risk to your small and medium business customers, competitively priced to encourage awareness of cyber risk in their environments, which ultimately reduces the cyber risk to your business

MASTERCARD CYBERSECURITY SOLUTIONS



Mastercard's Capabilities & Expertise

Outputs

Area



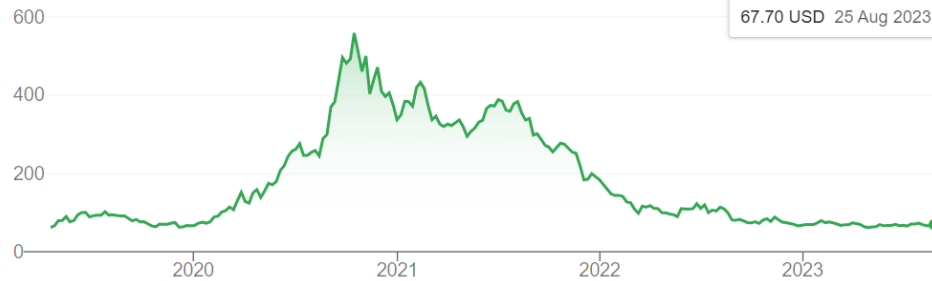
72.06 USD

+10.06 (16.23%) ↑ past 5 years

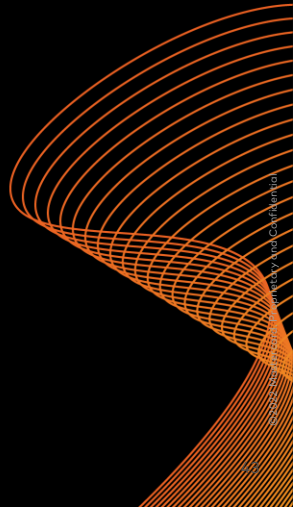
Closed: 8 Sept, 7:52 pm GMT-4 • Disclaimer

After hours 72.13 +0.070 (0.097%)

1D | 5D | 1M | 6M | YTD | 1Y | 5Y | Max

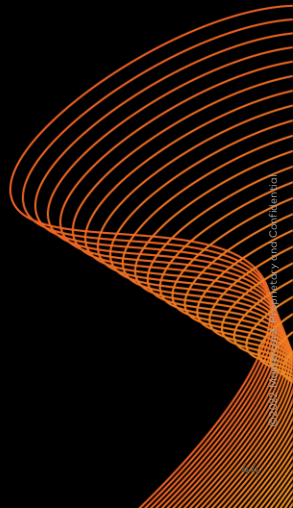


Open	73.68	Mkt cap	21.69B	52-wk high	89.67
High	73.80	P/E ratio	754.71	52-wk low	60.45





**ITS NOT ABOUT THE TREES,
ITS ABOUT THE FOREST**



Contact information

Learn more about Mastercard's work in cybersecurity by reaching out to your Mastercard representative or contact below:

Mandeep Sedha

Director, Product Management, Cyber & Intelligence,
Mastercard
Mandeep.Sedha@mastercard.com

Deric Karunesudas

Director, Cyber Security, Data & Services
Mastercard
Deric.Karunesudas@mastercard.com

