RESOLVE SYSTEMS™

The Definitive Guide to Cybersecurity in Singapore

4 Things You Need to Know About the New Singapore Cybersecurity Bill

Table of Contents

Glossary

Cyber Security Agency of Singapore (CSA) - Formed in April 2015 under the Prime Minister's Office, it is the national agency overseeing cybersecurity strategy, operations, education, outreach, and ecosystem development.
Critical Information Infrastructures (CII) – A computer or computer system necessary for continuous delivery of essential services which Singapore relies on; the loss or compromise of which will lead to a debilitating impact on national security, defense, foreign relations, economy, public health, public safety, or public order of Singapore.
Computer Misuse and Cybersecurity Act (CMCA) - An Act for securing computer material against unauthorized access or modification. Provides authority to measure and ensure cybersecurity.
National Cyber Security Center (NCSC) – Monitors and analyzes cyber threat landscape to maintain cyber situational awareness and anticipate future threats.
Ministry of Communications and Information (MCI) – Oversees the development of the infocomm media, cybersecurity, and design sectors of Singapore.

Who's Who in Singapore

Mr. Lee Hsien Loong - Prime Minister of Singapore
Mr. David Koh – Singapore's Defense Cyber Chief leading Defense Cyber Organization
Mr. Teo Chee Hean - Deputy Prime Minister and Coordinating Minister for National Security
Dr. Yaacob Ibrahim - Minister for Communications and Information; Minister-in-charge of Cyber Security

Executive Summary

Singapore is a highly digitized country and is only becoming more so as they expand upon their goal of being a Smart Nation. Smart Nation is the national effort of Singaporeans, businesses, and government to support better living using technology with advancements in transport, home and environment, business productivity, health services, and public sector services.

"Smart Nation is about Singapore taking full advantage of IT. Using IT comprehensively to create new jobs, new business opportunities, to make our economy more productive, to make our lives more convenient."

Prime Minister Lee Hsien Loong
National Day Rally
August 20, 2017[3.1]

While becoming a Smart Nation, cybersecurity threats and subsequent cybercrime are still on the rise. Security Operations Centers (SOCs) are more at risk than ever before. With companies constantly battling incidents – from Bad Rabbit to WanaCrypt0r – the government is advancing legislation with a new cybersecurity Omnibus bill.

With challenges in security incident processes, skill shortages, unauditable manual triage, and finite personnel, the Singapore government is expanding their Cyber Security Agency (CSA) with new legislation. Currently focused on coordinating strategy, the overarching Omnibus bill will have additional measures to standardize and protect Critical Information Infrastructures (CII).

Continue reading this eBook for the history of cybersecurity, need for legislation, the key parts of the Omnibus bill, and how Resolve Systems can help compliance by providing playbooks, process orchestration, and collaborative incident response and resolution.

40% of all economic crime in Singapore is cybercrime[3.2]

History of Cybersecurity Legislation in Singapore

As the current leader in the Global Cybersecurity Index rankings[4.1], Singapore has earned the title due to significant focus and funding on legislation improvements. With a master plan created as far back as 2005, Singapore has refined and expanded legislation on cybersecurity, and fighting cybercrime, in the last two years.

Dating back to April 1, 2015, when Singapore was sixth on the Global Security Index, the Cyber Security Agency (CSA) was created. The CSA is responsible for the national protection of cybersecurity and computer systems, from detection to response and recovery, from cyber threats and incidents[4.2]:

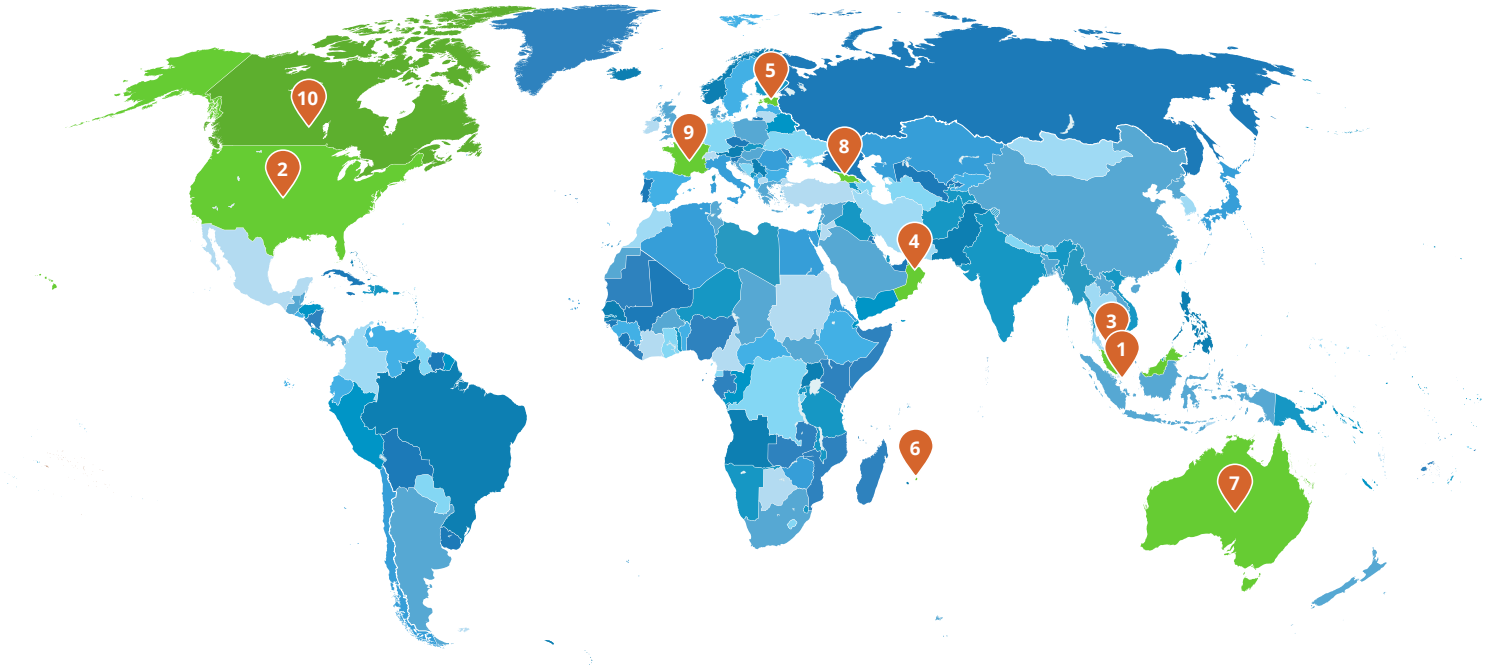
- Secure a computer/computer system against unauthorized access or malicious acts
- Preserve the availability and integrity of the computer or computer system and confidentiality of information stored or processed in the computer or computer system

Global Cybersecurity Index Ranking 2017

Source: UN International Telecommunication Union Straits Times Graphics

Country	GCI Score*	2017 Ranking	2015 Ranking
Singapore	0.92	1	6
United States	0.91	2	1
Malaysia	0.89	3	3
Oman	0.87	4	3
Estonia	0.84	5	5
Mauritius	0.82	6	9
Australia	0.82	7	3
Georgia	0.81	8	12
France	0.81	9	9
Canada	0.81	10	2

*Normalized



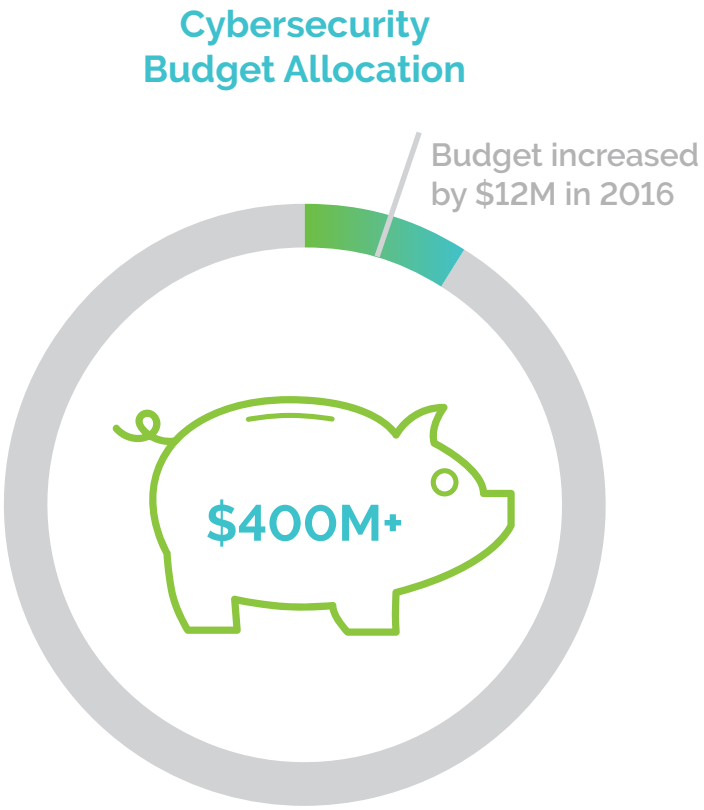
History of Cybersecurity Legislation in Singapore, *cont.*

Two years after the formation of the CSA and the Computer Misuse and Cybersecurity Act (which focused predominantly on cybercrime), more comprehensive legislation was written to address the ever evolving threat landscape.

To protect the Critical Information Infrastructures (CII), the CSA announced a new strategy in October 2016 nearly doubling the percentage of the technology budget to plug security gaps in critical infrastructure[5.1]. Singapore spent 5% of the infocomm technology (ICT) budget on cybersecurity – more than $400 million in fiscal 2014[5.2] – which was increased in 2016 to 8% to support the strategy.

Expanding upon this, the CSA worked for two years on an Omnibus bill – encompassing more than the CMCA bill – which requires more extensive measures to enhance the cybersecurity of CIIs. Announced in 2016, the bill was open for public review July 10, 2017 and will be enacted by Parliament in 2018[5.3].

Infocomm Technology (ICT) Budget



2014-2016

Vision of a Smart Nation: Timeline of Cybersecurity Legislation in Singapore

2005

Singapore first launches a cyber security masterplan[6.1]

2015

April 1: The Cyber Security Agency (CSA) of Singapore is created[6.1]

2016

October 10: Cybersecurity Strategy is announced at the Singapore International Cyber Week[6.2] with four key strategies in mind:

1. Building a Resilient Infrastructure
2. Creating a Safer Cyberspace
3. Developing a Vibrant Cybersecurity Ecosystem
4. Strengthening International Partnerships

2017

April: Hackers breach the networks of the National University of Singapore and Nanyang Technological University. They were able to steal government-related data including defense projects, foreign affairs, and transport sector information.

July 10: Cybersecurity Bill is disclosed to the public, which aims to provide the Cyber Security Agency of Singapore (CSA) with the powers to manage and respond to cybersecurity threats.

September 18: Delay in the Cybersecurity Bill being introduced to Parliament[6.3].

2018 & Beyond

New Omnibus cybersecurity bill is in effect with new roles to ensure compliance. Security incidents will be reported to the government within hours; enterprises will need to have a process orchestration and security incident response plan in place to ease compliance.

RESOLVE SYSTEMS™

Need for Legislation

Even though Singapore leads the world in cybersecurity, threats are on the rise locally and globally. With demand to keep up with attacks and breaches, and to secure the #1 spot for years to come, the proposed legislation will help solve many issues plaguing CISOs and security operations teams.

With cybersecurity attacks more prevalent and also more costly each year – including 2017's WannaCry and Petya – Singapore is being proactive to keep up with hackers. Mr. Koh, CSA's Chief Executive, said "Around the world we have seen attacks affecting critical infrastructure such as energy and power supply." Though critical sectors weren't affected by the ransomware attacks in 2017, Singapore is still at risk.

80% of Singapore organizations are confident in their ability to detect a sophisticated cyber attack[7.1]: those same organizations don't believe their cybersecurity plan meets their organization's need.

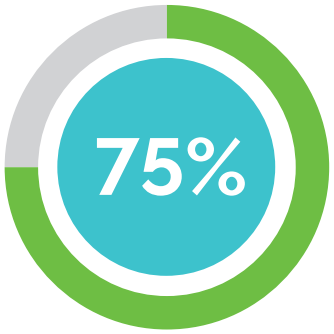
Obstacles of Securing Information in Singapore[7.1]

Lack of Skilled Sources

Budget Constraints

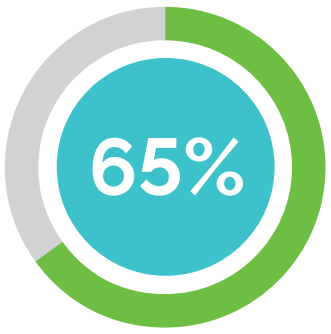
Lack of Quality Tools for Managing Information

Top Cybersecurity Concerns for Singapore[7.1]



Data Leakage and Loss Prevention

Security Testing for Attack and Penetration



Identity and Access Management

Need for Legislation – Struggles of Cybersecurity

Where are Singapore CISOs and CIOs struggling when it comes to cybersecurity?

With increased digitization and reliance on IoT, cloud based business models, and email as a main source of communication, the threats continue to increase. Expanding legislation to address the increasing threat volume, Singapore is acknowledging cybersecurity breaches are no longer a matter of *if* but, in today's reality, *when*.

According to PriceWaterhouseCooper (PwC), phishing is still Singapore's most prevalent cybersecurity and privacy threat[8.1]. In the last year, a fifth of Singapore organizations experienced more than 3 major incidents and 13% experienced *more than* 500 security incidents!

Security threats aren't just contained to phishing. PwC also reported where incident(s) occur:

To reduce vulnerabilities, the upcoming Omnibus bill outlined ways to detect, respond, and resolve incidents with training, budget allocation, and stronger measures. Let's review the key parts of the legislation and where organizations can prepare to respond to cyber attacks.

Objectives of the Omnibus Bill

Announced for public review July 10, 2017, the Cyber Security Agency (CSA) of Singapore has been preparing overarching and sweeping legislation for two years. Going into effect in 2018, this bill has four key objectives[9.1]:

1. Provide a framework and formalize ownership roles for the regulation of Critical Information Infrastructures (CII).

2. Expand the current Computer Misuse and Cybersecurity Act (CMCA) by providing the CSA with the ability and oversight to manage and respond to cybersecurity threats and incidents.

> **"As the (threat) landscape evolves, it is better to have an omnibus bill that oversees the cybersecurity of (essential services) as a whole."**
>
> Mr. David Koh
> CSA Chief Executive
> July 10, 2017

3. Create a framework to share and protect cybersecurity information with the CSA.

4. Establish light-touch licensing framework for cybersecurity service providers.

With a holistic approach to making Singapore resilient against cyber attacks and to ensure preparation, effectiveness, and timely response when attacks happen, this bill expands upon existing laws and regulations.

To achieve the desired outcome of a consistent cybersecurity framework across multiple sectors, and beyond the Personal Data Protection Act (PDPA), a broader omnibus cybersecurity bill is needed for Singapore to join the ranks of Germany and the Czech Republic (with omnibus laws). Let's review the key parts of Singapore's omnibus legislation now.

Key Parts of the Singapore Omnibus Legislation

With ongoing concern on cybersecurity threats and incidents on the rise globally and locally, Singapore has outlined specific protection, particularly for CII. The most important facets are outlined below.

#1 Oversight and maintenance of national cybersecurity – including financial services

The Singapore government believes they are only as strong as their weakest link and wrote the Omnibus legislation accordingly. The bill is focused on a coordinated, consistent national approach to level up across all critical sectors – both public and private – to protect CII.

Organizations must share information to facilitate investigation of any threat or incident. To protect CII consistently, a mandate of common framework across all sectors, including financial services, is meant to empower CSA officers to investigate cybersecurity threats and incidents.

The bill will supersede current banking and privacy rules for any serious threat.

Based on Section 21 of the bill, a cybersecurity threat or incident is deemed serious if it meets the following risk criteria:

1. Significant harm to CII
2. Disrupting an essential service
3. Threat to Singapore's national security, defense, foreign relations, economy, or public health, order, or safety
4. Severe harm to valuable information, whether or not the computer or computer systems are technically part of critical information infrastructure (CII)

> **"The bill, as it stands, is bold, decisive, and forward looking in considering the threats posed by cyber attacks on Singapore's essential services."**
>
> Mr. Gerry Chng
> EY Asean Cyber Security Leader
> Ernst & Young Advisory Pte. Ltd.
> July 10, 2017

Always flexible and taking into account the unique sectors, CSA officers are also further empowered to enforce this framework.

#2 Empower the CSA to Carry out Respected Functions

The new bill also mandates new roles and responsibilities to support the expanded protections.

A new Commissioner of Cybersecurity, appointed by the Minister-in-Charge, will be the new Chief Executive of the CSA. This role extends the government's ability and approach by giving CSA officers and sector leads additional bandwidth, empowering them to investigate incidents. These authorized officers will be responsible for enforcing the bill publicly and privately.

When the Commissioner learns of a cybersecurity threat or incident, he has the choice to investigate with these objectives in mind:

1. Determine the impact of the threat

2. Prevent significant harm from a breach or incident

3. Reduce additional incidents from arising or progressing from the initial threat or incident

When specialized technical knowledge is required, the Commissioner also has the authority to appoint special advisers and officers. These experts can be either public or private as long as they are the *most* qualified with the computer system. They will be commissioned to aide in the investigation.

In the unfortunate situation of a breach or incident, all organizations and CII owners suffering a cybersecurity attack must notify the Commissioner. The duties of CII owners have also expanded to ensure compliance and protection of their owned computer or computer systems.

"It is a matter of (time before) cybersecurity incidents happen here. This cybersecurity bill will provide a good foundation for Singapore to manage cybersecurity risk."

Mr. Vincent Loy
PwC Singapore's Asia-Pacific Cybercrime and Financial Crime Leader

#3 Proactive Approach with Designated CII Owners (CIIOs)

Outlined in sections 11-17 is an approach to assess risk profiles of critical information infrastructure (CII) to reduce the impact of cybersecurity incidents when they happen. Due to differing technologies and maturation of industry experts, the Omnibus bill recognizes every CII sector as different – from private to government – and assigns specific ownership to CII Owners (CIIOs).

#3 Proactive Approach with Designated CII Owners (CIIOs) *cont.*

CIIOs are responsible for the cybersecurity of their CIIs with specific statutory duties outlined in Section 10, including the duty to:

- Provide information to the Commissioner on technical architecture of the CII
- Comply with practice codes and direction of the Commissioner
- Report incidents to the Commissioner of any cybersecurity incident affecting their CII
- Conduct compliance audits and risk assessments
- Participate in cybersecurity exercises

The CSA will provide more guidance on how CIIOs comply with these duties; failure to do so (without reasonable excuse) will be a criminal offense. Due to national security implications, it's the failure to comply which is criminal.

#4 Investigate and Respond to Cybersecurity Threats and Incidents

Though it's the CIIO's job to make sure the computer is well-protected, serious threats need to be contained, assessed, and resolved to prevent more serious consequences.

CSA officers, CIIOs, the Commissioner, and delegated Assistant Commissioners will have the power to investigate threats to respond quickly. There are three scenarios where mandated reporting and response will occur:

1. **Section 20**: All cybersecurity threats and incidents
   - The Commissioner may examine and take statements (with technical logs) from anyone relevant to the investigation to decide the severity of the incident.
2. **Section 21**: Serious cybersecurity threats and incidents
   - The Commissioner may exercise more intrusive measures than Section 20 to assist in investigations, scan for vulnerabilities, or even potentially seize computers for further examination.
3. **Section 24**: Emergency measures and requirements
   - With a certificate, the Minister can authorize any person or organization to take any measure to prevent, detect, and/or counter any threat to a computer

Read the bill in its entirety on CSA's website here.

How can CISOs and SOCs prepare for this legislation?

Resolve Systems can help.

Resolve Systems' Security Incident Response Platform to Help CIIOs

"The ability to accomplish Singapore's smart nation vision not only hinges on identifying and implementing the right technology with adequate safeguards to protect privacy and confidentiality, but also the soft skills to ensure that the right processes are in place to maintain the operations of such complex systems."

Freddy Tan
Vice President of the Association of Information Security Professionals (AISP) in Singapore[13.1]

Singapore is a highly connected country with daily cybersecurity incidents. While most are inconsequential, there are some serious threats with real risk to CIIs, Singapore's national security, or computers and people.

How can you do more with what you have and remain compliant to the new legislation and growing cyber threats? Resolve Systems knows the answer: establish a security incident response plan and implement Resolve, an automation and process orchestration platform.

Historically, organizations have made investments in detection and investigation technologies which flood analysts with a high volume of incidents and ultimately lead to alert fatigue. In addition to the increased level of escalations to security experts, other challenges in the SOC include too many false alerts, inefficient cross-team collaboration, and manual and adhoc incident response processes for investigation and case management.

Prepare for a serious breach. Not handling incidents quickly could cost Singapore companies with irreversible damage to IT infrastructure or a company's brand, and also hefty fines and potential imprisonment with the outlined legislation.

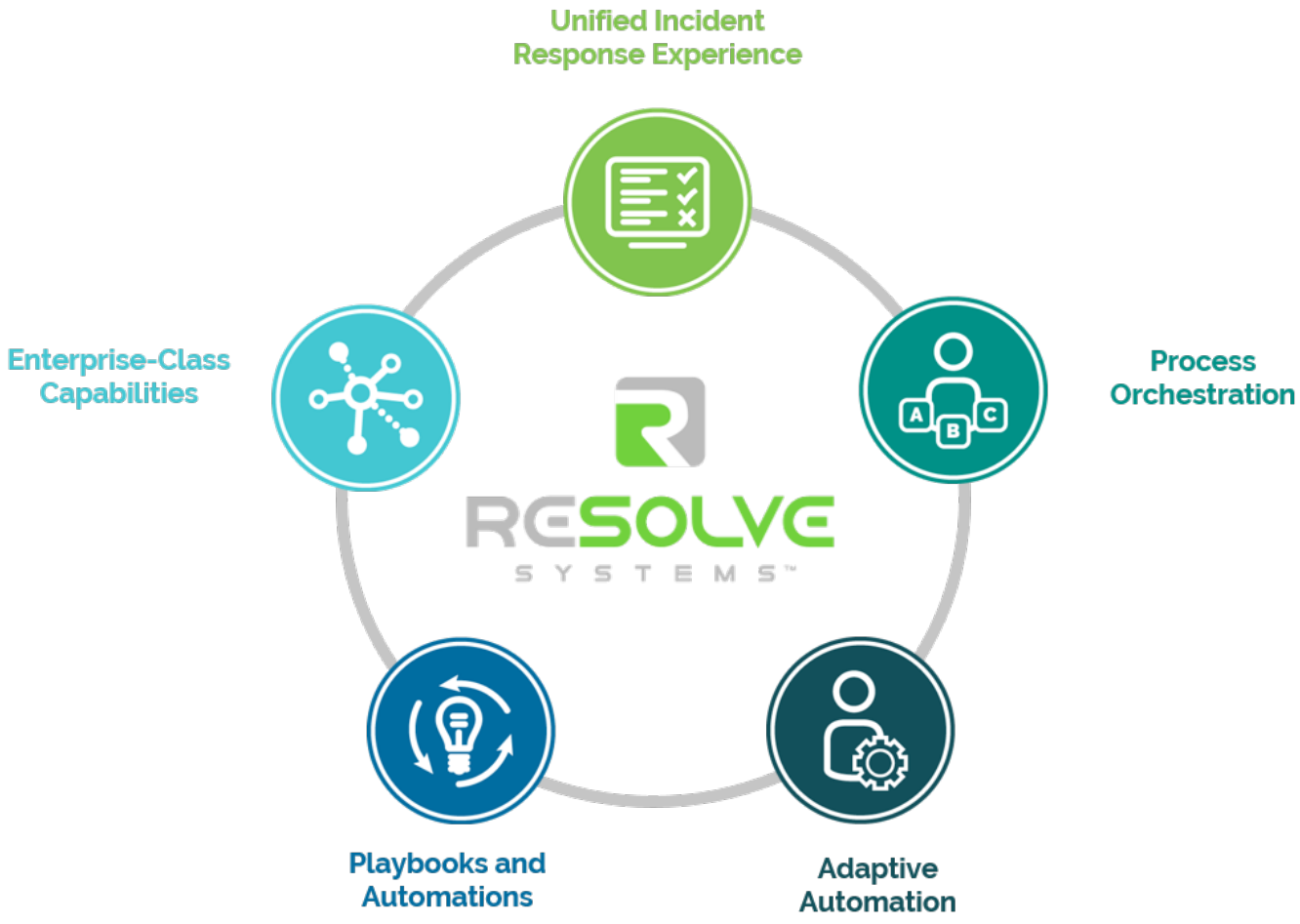
Enterprises and CISOs are looking to security incident response, orchestration, and automation technologies to help bridge this skills gap and prioritize alerts.

Resolve Systems provides the only enterprise-wide platform for collaborative work across IT operations, Network operations, and Security operations teams to accelerate incident response and protect Singapore.

Conclusion

With the outlined measures of the Omnibus bill to detect, respond, and resolve incidents, Resolve Systems is ready to enable SOCs with enterprise-wide security incident response automation and orchestration software. Work faster, smarter, and more efficiently by empowering experts with a unified incident response platform for all tasks, processes, automation, and note keeping. CIIs and their respective owners will have access to playbooks, process guidance, human-guided and end-to-end automation to respond to and resolve all incidents while having notes to report back to the Commissioner of Singapore.

For more information on the leading security incident response platform, contact Resolve Systems now.



About Resolve Systems

Resolve Systems provides the most widely-deployed enterprise IT, network, and security incident response automation and orchestration platform, Resolve. Resolve accelerates incident response and resolution via adaptive automation and enterprise-wide process orchestration. Trusted by more Fortune 500 organizations than any other platform, Resolve helps speed response and resolution for security, network, and IT incidents via the right prescriptive guidance, interactive processes, and intelligent automation to maximize operations staff's leverage throughout the incident life cycle.

Headquartered in Irvine, California, USA with operations in EMEA and APAC, Resolve Systems has been successfully deployed at scale by more than 100 of the largest global Enterprises. Resolve Systems is majority owned by Insight Venture Partners, the leading high-growth global private equity firm.

About Insight Venture Partners

Insight Venture Partners is a leading global venture capital and private equity firm investing in high-growth technology and software companies that are driving transformative change in their industries. Founded in 1995, Insight has raised more than $13 billion and invested in nearly 300 companies worldwide. Our mission is to find, fund and work successfully with visionary executives, providing them with practical, hands-on growth expertise to foster long-term success. For more information on Insight and all of its investments, visit www.insightpartners.com.

References

(3.1) http://www.pmo.gov.sg/national-day-rally-2017

(3.2) https://www.pwc.com/sg/en/consulting/assets/economic-crime-survey/economic_crime_survey_2016_singapore.pdf

(4.1) https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

(4.2) http://www.straitstimes.com/singapore/spore-rolls-out-high-level-cyber-security-strategy

(6.1) http://www.straitstimes.com/tech/spore-takes-top-spot-in-un-cyber-security-index

(6.2) https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy#sthash.hLf26Zll.dpuf

(6.3) http://www.straitstimes.com/singapore/new-bill-proposed-to-beef-up-cyber-security

(7.1) http://www.ey.com/sg/en/newsroom/news-releases/news-ey-singapore-companies-confident-of-predicting-and-resisting-cyber-attacks

(7.2) http://www.straitstimes.com/singapore/new-bill-proposed-to-beef-up-cyber-security

(8.1) Global State of Information Security® Survey 2017 Singapore highlights- PricewaterhouseCooper, 2017 https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/internet-of-things.html

(9.1) Public Consultation Document, Singapore Cyber Security Agency, July 2017. https://www.reach.gov.sg/participate/public-consultation/ministry-of-communications-and-information/public-communications-division/public-consultation-paper-on-the-draft-cybersecurity-bill

(13.1) http://www.computerweekly.com/news/4500277583/Cyber-security-professionals-in-Singapore-could-get-20-pay-rise

North American Headquarters
2302 Martin Street, Suite 225
Irvine, CA 92612
T: +1.949.325.0120

Asia Pacific Headquarters
02-01, One Fullerton
Singapore, 049213
T: +65 68325513

EMEA Headquarters
60 Cannon St, Suite 119
London EC4N 6LY, UK
T: +44 (20) 37432123