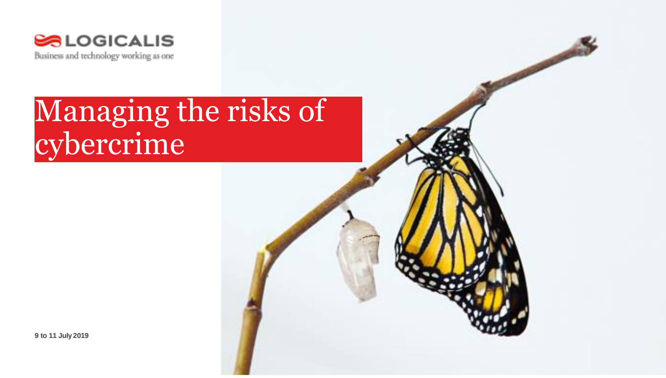
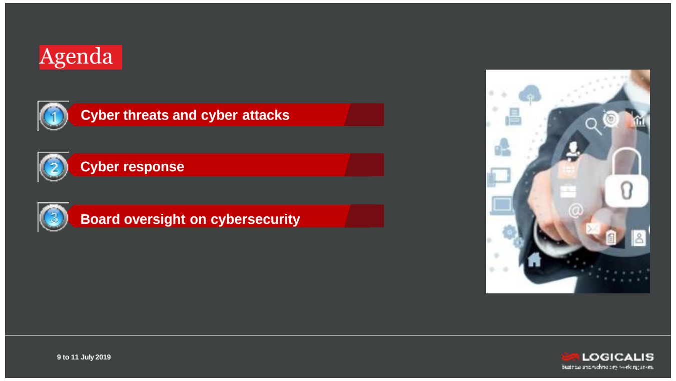


LOGICALIS
Business and technology working as one

Managing the risks of cybercrime

9 to 11 July 2019

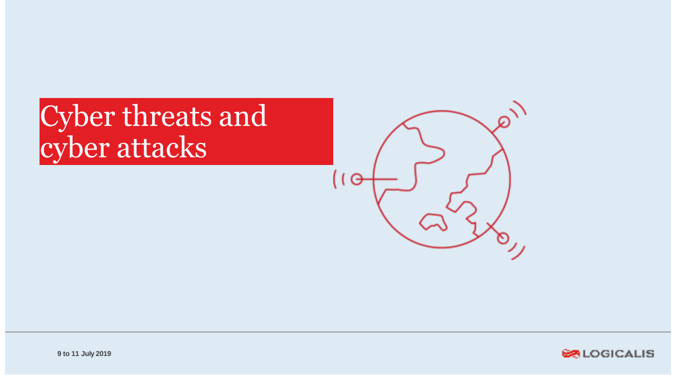


Agenda

1. Cyber threats and cyber attacks
2. Cyber response
3. Board oversight on cybersecurity

9 to 11 July 2019

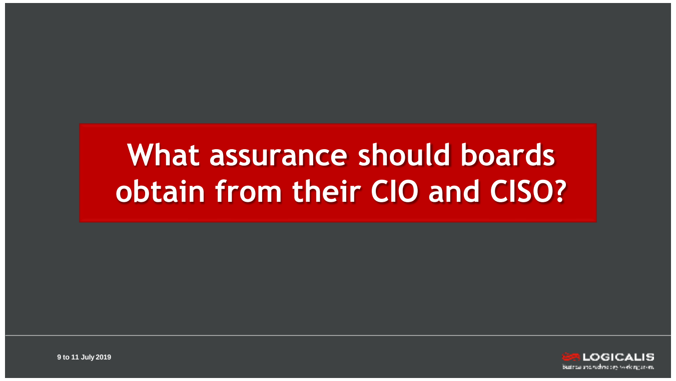
LOGICALIS
Business and technology working as one



Cyber threats and cyber attacks

9 to 11 July 2019

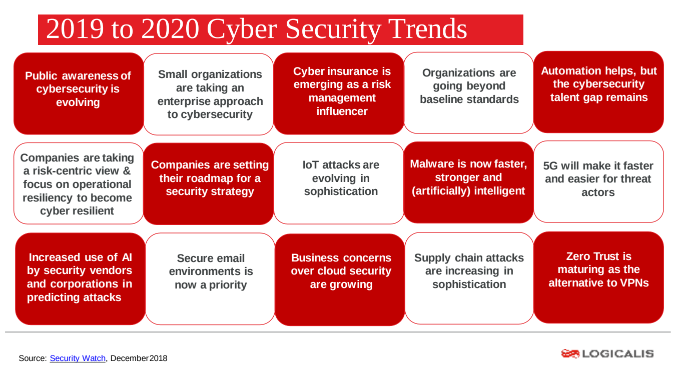
LOGICALIS



What assurance should boards obtain from their CIO and CISO?

9 to 11 July 2019

LOGICALIS



2019 to 2020 Cyber Security Trends

Public awareness of cybersecurity is evolving	Small organizations are taking an enterprise approach to cybersecurity	Cyber insurance is emerging as a risk management influencer	Organizations are going beyond baseline standards	Automation helps, but the cybersecurity talent gap remains
Companies are taking a risk-centric view & focus on operational resiliency to become cyber resilient	Companies are setting their roadmap for a security strategy	IoT attacks are evolving in sophistication	Malware is now faster, stronger and (artificially) intelligent	5G will make it faster and easier for threat actors
Increased use of AI by security vendors and corporations in predicting attacks	Secure email environments is now a priority	Business concerns over cloud security are growing	Supply chain attacks are increasing in sophistication	Zero Trust is maturing as the alternative to VPNs

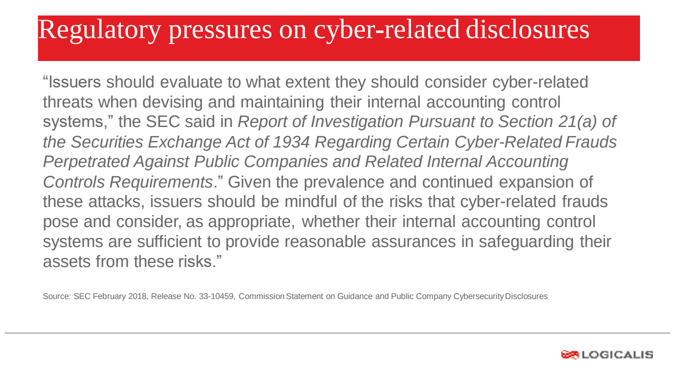
Source: Security Watch, December2018

LOGICALIS

By 2020, 100% of large enterprises will be asked to report to their Board of Directors on cybersecurity (Gartner, 2018)

9 to 11 July 2019

LOGICALIS



Regulatory pressures on cyber-related disclosures

"Issuers should evaluate to what extent they should consider cyber-related threats when devising and maintaining their internal accounting control systems," the SEC said in *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements*." Given the prevalence and continued expansion of these attacks, issuers should be mindful of the risks that cyber-related frauds pose and consider, as appropriate, whether their internal accounting control systems are sufficient to provide reasonable assurances in safeguarding their assets from these risks."

Source: SEC February 2018, Release No. 33-10459, Commission Statement on Guidance and Public Company Cybersecurity Disclosures

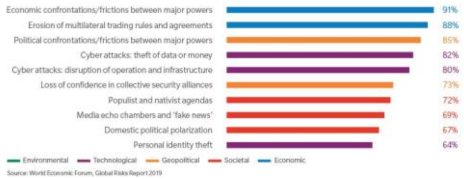
LOGICALIS

Cyber security features as a high risk in the World Economic Forum 2019 Global Risk Report

9 to 11 July 2019

LOGICALIS
business and technology working as one

World Economic Forum high risks



Source: World Economic Forum, Global Risks Report 2019

Global risks

LOGICALIS

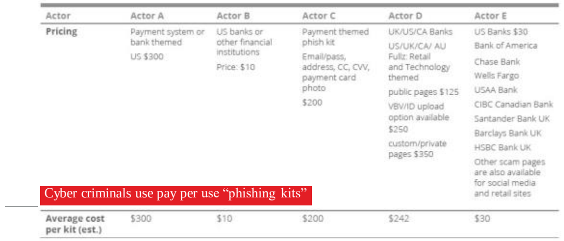
Cyber threats and cyber risks remain uncharted territory for many enterprises

9 to 11 July 2019

Cyber Crime is “financially attractive” to threat actors

Cyber criminal businesses can be operated for as little as $34 month with a profit of $25,000 per month. Advanced cyber criminals may routinely require nearly $3,800 per month with a profit of $1 million per month.

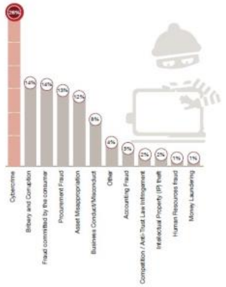
Source: Deloitte, December 2018



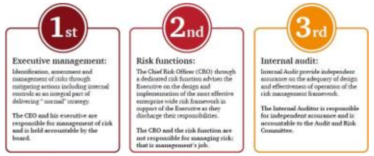
Actor	Actor A	Actor B	Actor C	Actor D	Actor E
Pricing	Payment system or bank themed US $300	US banks or other financial institutions Price: $10	Payment themed phish kit Email/pass, address, CC, CVV, payment card photo $200	UK/US/CA Banks US/UK/CA/ AU Fullz: Retail and Technology themed public pages $125 VBV/ID upload option available $250 custom/private pages $350	US Banks $30 Bank of America Chase Bank Wells Fargo USAA Bank CIBC Canadian Bank Santander Bank UK Barclays Bank UK HSBC Bank UK Other scam pages are also available for social media and retail sites
Average cost per kit (est.)	$300	$10	$200	$242	$30

Cyber criminals use pay per use “phishing kits”

Disruptive economic crimes in next 24 months



Boards need to use these lines of defence



1st **Executive management:** Identification, assessment and management of risks through mitigating actions including internal controls as an integral part of delivering " normal" strategy.

The CEO and his executive are responsible for management of risk and is held accountable by the board.

2nd **Risk functions:** The Chief Risk Officer (CRO) through a dedicated risk function advises the Executive on the design and implementation of the most effective enterprise wide risk framework in support of the Executive as they discharge their responsibilities.

The CRO and the risk function are not responsible for managing risk: that is management's job.

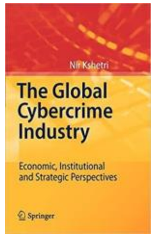
3rd **Internal audit:** Internal Audit provide independent assurance on the adequacy of design and effectiveness of operation of the risk management framework.

The Internal Auditor is responsible for independent assurance and is accountable to the Audit and Risk Committee.

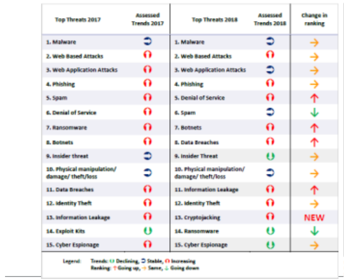
Source: PwC, Global Economic Crime and Fraud Survey, 6th South African edition February 2018

Cyber crime is global, lucrative & threatening

- Large scale
- Multi products and vendors
- E-Commerce marketplaces
- Training and technical support
- Collaboration forums
- Advertisements

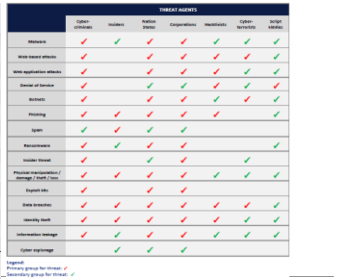

Nir Kshetri
The Global Cybercrime Industry
Economic, Institutional and Strategic Perspectives
Springer

Observations on cyber attacks



Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	⊃	1. Malware	⊃	→
2. Web Based Attacks	∩	2. Web Based Attacks	∩	→
3. Web Application Attacks	∩	3. Web Application Attacks	⊃	→
4. Phishing	∩	4. Phishing	∩	→
5. Spam	∩	5. Denial of Service	∩	↑
6. Denial of Service	∩	6. Spam	⊃	↓
7. Ransomware	∩	7. Botnets	∩	↑
8. Botnets	∩	8. Data Breaches	∩	↑
9. Insider threat	⊃	9. Insider Threat	∪	→
10. Physical manipulation/ damage/ theft/loss	⊃	10. Physical manipulation/ damage/ theft/loss	⊃	→
11. Data Breaches	∩	11. Information Leakage	∩	↑
12. Identity Theft	∩	12. Identity Theft	∩	→
13. Information Leakage	∩	13. Cryptojacking	∩	NEW
14. Exploit Kits	∪	14. Ransomware	∪	↓
15. Cyber Espionage	∩	15. Cyber Espionage	∪	→

Legend: Trends: ∪ Declining, ⊃ Stable, ∩ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down



	THREAT AGENTS						
	Cyber-criminals	Insiders	Nation States	Corporations	Hacktivists	Cyber-terrorists	Script kiddies
Malware	✓	✔	✓	✓	✔	✔	✔
Web based attacks	✓		✓	✓	✓	✓	✔
Web application attacks	✓		✓	✓	✓	✔	✔
Denial of Service	✓		✔	✔	✓	✔	✓
Botnets	✓		✓	✓	✔	✓	✔
Phishing	✓	✓	✓	✓	✓		✔
Spam	✔	✓	✔	✔			
Ransomware	✓	✔	✓	✓			✔
Insider threat	✓		✔	✓		✔	
Physical manipulation / damage / theft / loss	✓	✓	✓	✓	✔	✔	✔
Exploit kits	✓		✓	✓			
Data breaches	✓	✓	✓	✓	✓	✓	✔
Identity theft	✓	✓	✓	✓	✓	✔	✔
Information leakage	✓	✔	✓	✓	✔	✔	✔
Cyber espionage		✔	✔	✔			

Legend:
Primary group for threat: ✓
Secondary group for threat: ✔

Observations on cyber attacks

Advances in Command and Control (C2) communication

Malware authors increasingly targeting IoT devices

The mobile malware landscape is steadily increasing

Cyber criminals are moving from ransomware to cryptojacking

Fileless attack techniques are the new norm

APTs, malware campaigns and potential usage of watering-hole attacks

New financial malware with new web-based capability

Web browser based (drive-by) exploit-kits is continuing

SQL injection continues to lead the attacks types

Legacy web application exploits are still among the top 20+

Phishing attacks became more targeted

Rapid increase in phishing sites using HTTPS

DDoS and geo-politics landscape

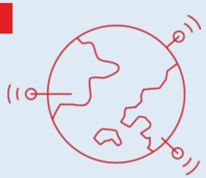
Multi-vector DDoS attacks

Encrypted DDoS attacks

Observations on cyber attacks

Data is exposed or compromised every day	Costs of a cybersecurity breach are high	Insider threat perception changed with GDPR	Digital theft has overtaken physical theft with respect to corporate fraud	Adoption of cloud storage
Human error is the most crucial factor for data disclosure	The cloud is an attack surface for customers' data	The prevalence of anonymous cryptocurrencies	Cryptocurrencies' market price and cryptojacking detections correlation	Ransomware 'DIY' is now readily available

Cyber response



9 to 11 July 2019

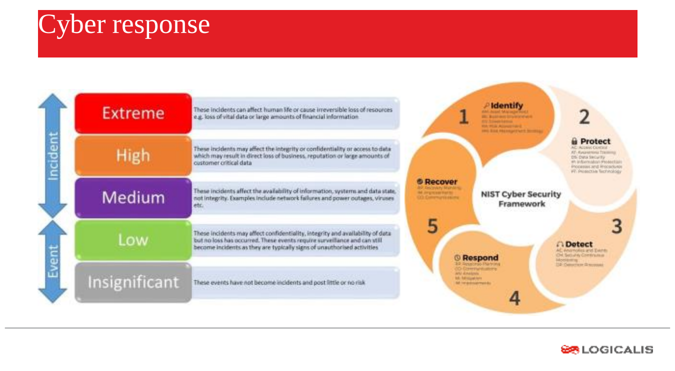
The dreaded headline news!!

Business comes to a halt as all workstations are encrypted with the Ryuk ransomware which infects online back ups.

Leaked M& A information because of a poor control on a back up firewall sparks affected employee's outrage.

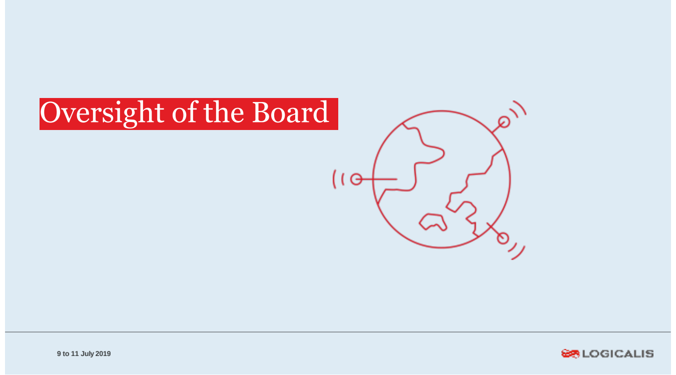
Undetected for two years, Command and Control servers are used for large scale botnet on the supplier portal.

Password Manager used by your Administrators is compromised which led to sensitive Board Members personal information being sold on the Darkweb.



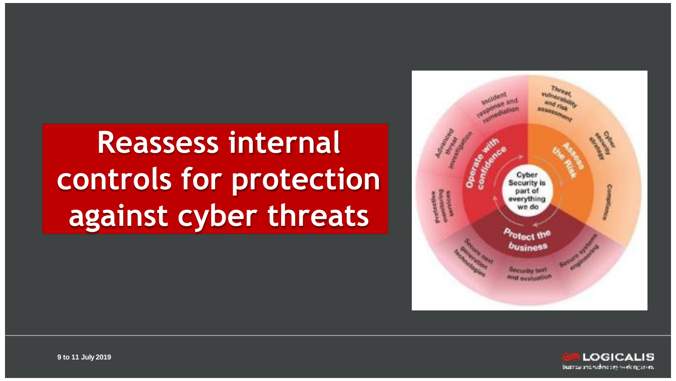
Cyber response

Incident	Extreme	These incidents can affect human life or cause irreversible loss of resources e.g. loss of vital data or large amounts of financial information
	High	These incidents may affect the integrity or confidentiality or access to data which may result in direct loss of business, reputation or large amounts of customer critical data
	Medium	These incidents affect the availability of information, systems and data state, not integrity. Examples include network failures and power outages, viruses etc.
Event	Low	These incidents may affect confidentiality, integrity and availability of data but no loss has occurred. These events require surveillance and can still become incidents as they are typically signs of unauthorised activities
	Insignificant	These events have not become incidents and post little or no risk



Oversight of the Board

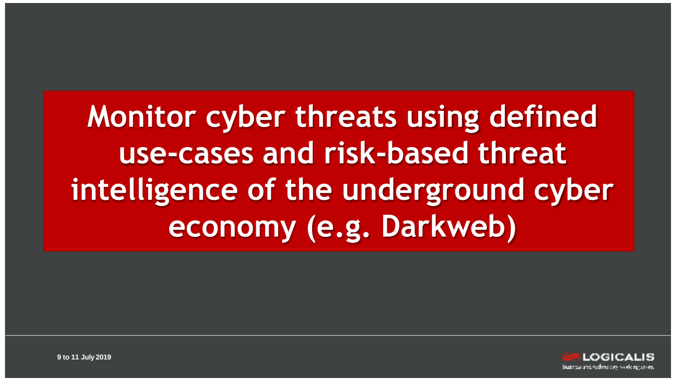
9 to 11 July 2019



Reassess internal controls for protection against cyber threats

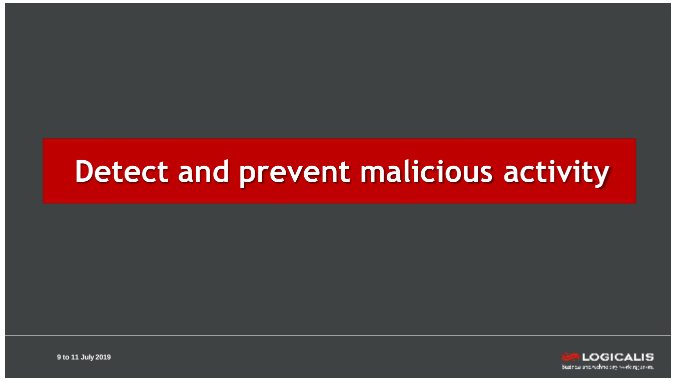
Cyber Security is part of everything we do
Assess the Risk
Protect the business
Operate with confidence
Threat, vulnerability and risk assessment
Cyber security strategy
Compliance
Secure systems engineering
Security test and evaluation
Secure next generation technologies
Protective monitoring services
Advanced threat investigation
Incident response and remediation

9 to 11 July 2019



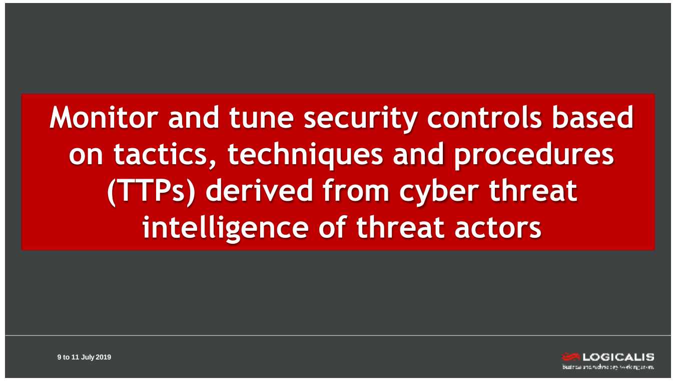
Monitor cyber threats using defined use-cases and risk-based threat intelligence of the underground cyber economy (e.g. Darkweb)

9 to 11 July 2019



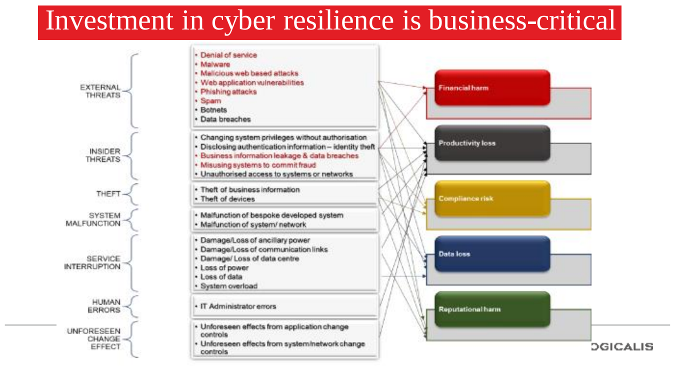
Detect and prevent malicious activity

9 to 11 July 2019



Monitor and tune security controls based on tactics, techniques and procedures (TTPs) derived from cyber threat intelligence of threat actors

9 to 11 July 2019



Investment in cyber resilience is business-critical

EXTERNAL THREATS
- Denial of service
- Malware
- Malicious web based attacks
- Web application vulnerabilities
- Phishing attacks
- Spam
- Botnets
- Data breaches

INSIDER THREATS
- Changing system privileges without authorisation
- Disclosing authentication information – identity theft
- Business information leakage & data breaches
- Misusing systems to commit fraud
- Unauthorised access to systems or networks

THEFT
- Theft of business information
- Theft of devices

SYSTEM MALFUNCTION
- Malfunction of bespoke developed system
- Malfunction of system/ network

SERVICE INTERRUPTION
- Damage/Loss of ancillary power
- Damage/Loss of communication links
- Damage/ Loss of data centre
- Loss of power
- Loss of data
- System overload

HUMAN ERRORS
- IT Administrator errors

UNFORESEEN CHANGE EFFECT
- Unforeseen effects from application change controls
- Unforeseen effects from system/network change controls

Financial harm

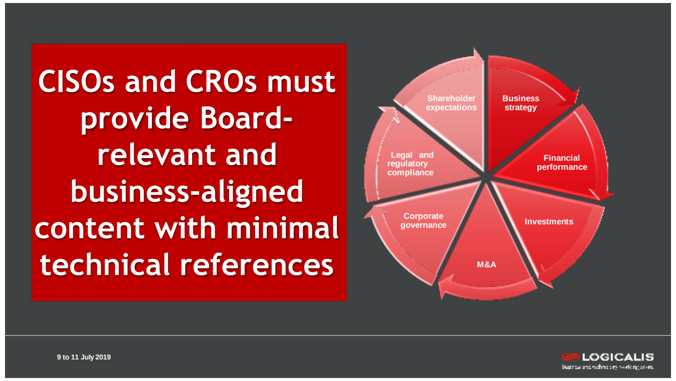
Productivity loss

Compliance risk

Data loss

Reputational harm

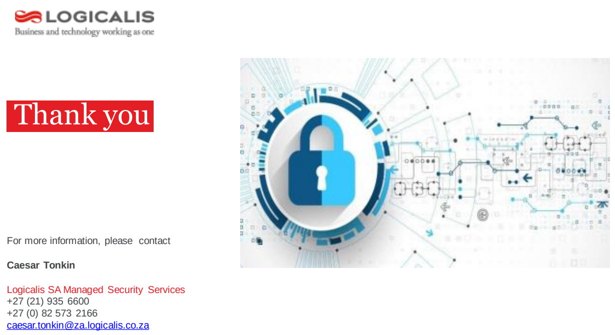
OGICALIS



CISOs and CROs must provide Board-relevant and business-aligned content with minimal technical references

9 to 11 July 2019

LOGICALIS



LOGICALIS
Business and technology working as one

Thank you

For more information, please contact

Caesar Tonkin

Logicalis SA Managed Security Services
+27 (21) 935 6600
+27 (0) 82 573 2166
caesar.tonkin@za.logicalis.co.za