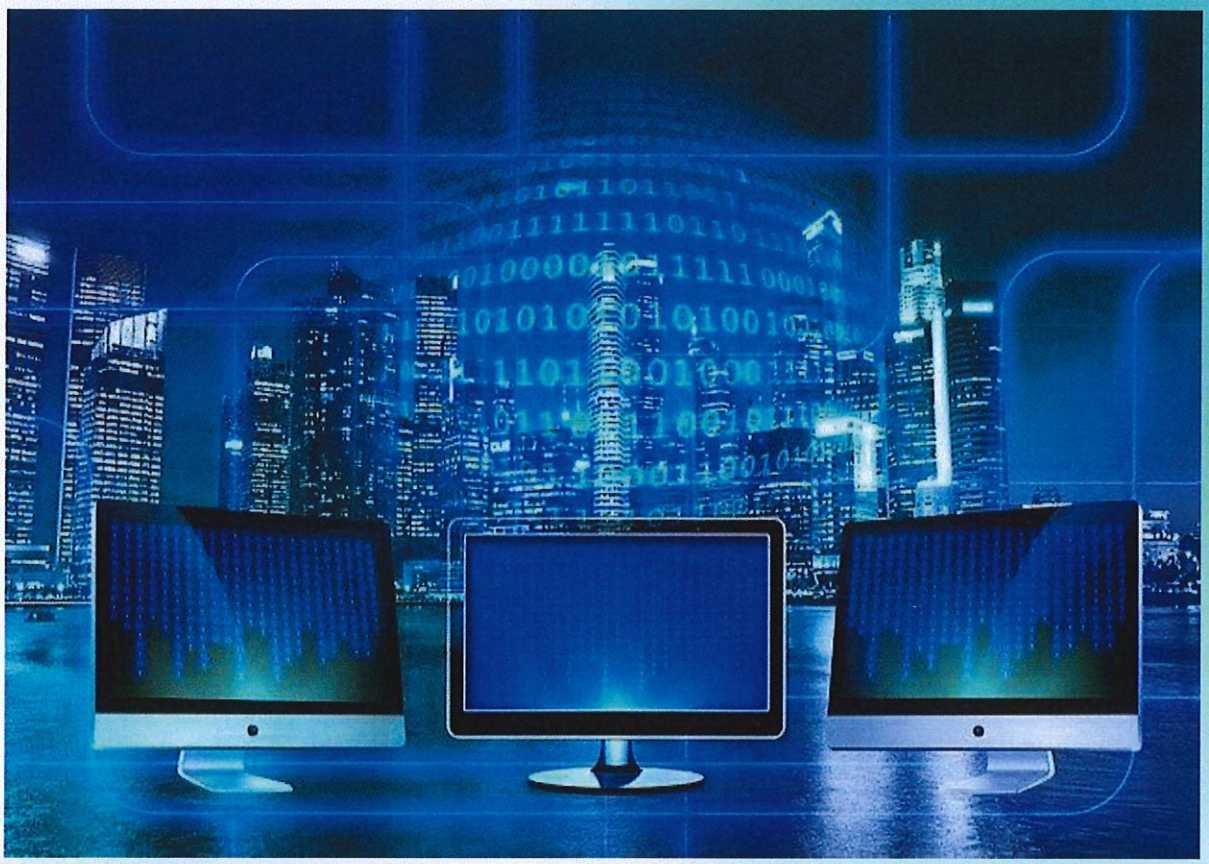


Parliament of Bermuda
Joint Select Committee

ON THE SEPTEMBER 2023 CYBER ATTACK ON THE GOVERNMENT OF BERMUDA

REPORT

Contents

Foreword from the Chair

As Chair of the Joint Select Committee appointed to examine the September 2023 cyber-attack on the Government of Bermuda, I present this report with a clear sense of responsibility to Parliament and to the people of Bermuda.

This report is not written for partisan advantage. It is written because cybersecurity is now a core part of public administration, public finance, personal privacy, national resilience, and trust in Government. The September 2023 incident demonstrated that a cyber-attack on Government systems is not simply an information technology issue. It can affect public services, payroll, communications, personal data, public confidence, national reputation, and the continuity of Government itself.

The Committee's work has been guided by two principles. First, the public deserves a clear and honest account of what happened, what was known before the attack, how Government responded, and what remains unresolved. Second, the value of this report must be measured not only by what it says about the past, but by whether it helps Bermuda prevent, withstand, and recover from future cyber incidents.

I wish to thank all persons, departments, agencies, organizations, and private-sector stakeholders who participated in the Committee's work, appeared before the Committee, answered questions, provided documents, or made written and oral submissions. Their contributions assisted the Committee in understanding the scale of the incident, the complexity of Government's recovery, and the reforms now required.

The Committee also recognizes the work of public officers, technical personnel, law enforcement, external specialists, and others who were involved in the immediate response and recovery effort. In a crisis of this nature, decisions often have to be made under pressure, with incomplete information and significant public expectation. That reality does not remove the need for accountability, but it does require the Committee to approach the evidence fairly and responsibly.

This report therefore seeks to strike the proper balance. It identifies warning signs, implementation gaps, governance weaknesses, public finance questions, and unresolved matters relating to data compromise and possible ransom-related expenditure. At the same time, it avoids reducing the issue to one individual, one Minister, one Department, one political party, or one administration.

The Committee's central message is forward-looking: Bermuda must treat cybersecurity as critical national infrastructure. Government must have clear accountability, dedicated funding, specialist staffing, tested recovery plans, Cabinet-level oversight, public communication protocols, and parliamentary tracking of implementation.

The September 2023 cyber-attack should be remembered not only as a disruption, but as a national warning. The purpose of this report is to ensure that the warning is acted upon.

Lawrence Scott, JP, MP Chair, Joint Select Committee on the September 2023 Cyber-Attack

Committee Membership

Lawrence Scott, JP, MP - Chair

Scott Simmons, JP, MP - Member

Jamahl S. Simmons, JP, MP - Member

Dwayne Robinson, JP, MP – Member

1. Executive Summary

This report presents an expanded parliamentary-style account of the September 2023 cyber-attack on the Government of Bermuda. It combines the Committee's original evidentiary narrative with a prevention- focused national resilience agenda. The Committee's central conclusion is that the incident should not be viewed only as an IT failure. It should be understood as a public administration, public finance, personal data, national resilience, and critical services event.

The Committee has not approached the September 2023 incident as an isolated technical event. Rather, it has considered the attack in the wider context of Government's increasing reliance on digital systems over a period of years, the evolution of cybersecurity governance, the pre-attack warning signs, the level of institutional readiness at the time the attack occurred, and the measures now required to reduce the likelihood and impact of future incidents.

The Committee is clear that the conditions that gave rise to Bermuda's 2023 cyber risk posture were not created by one political party, one Minister, one Department, or one administration. Bermuda's digital dependency increased under successive administrations led by both political parties. Cybersecurity awareness also increased over time. However, governance maturity, funding, specialist staffing, enterprise monitoring, disaster recovery, and cross-sector coordination did not consistently keep pace with the growth in digital reliance.

The most significant pre-attack evidence reviewed by the Committee is the May 2023 Cyberdine cybersecurity assessment. The materials reviewed indicate that approximately four months before the September 2023 attack, Government's cybersecurity risk posture was assessed as Critical. The assessment identified a high probability of successful cyber-attack and limited recovery capability, as well as root causes including resource constraints, gaps in strategic direction, and attack vectors such as ransomware, phishing, privacy breach, cloud-based breach, and third-party risk.

The Committee's assessment is that Government had begun a structured remediation programme prior to the attack. However, several foundational capabilities were not yet fully operational or mature at the time of the September 2023 incident. These included Security Operations Centre capability, Security Information and Event Management monitoring, ransomware defence, disaster recovery, backup programme maturity, and broader environment stabilization. The evidence therefore points to a gap between awareness of risk and full execution of mitigation measures.

The evidence reviewed by the Committee demonstrates that the September 2023 cyber-attack did not occur in the absence of warning. It occurred in the presence of documented risk, where corrective action had begun but had not yet been completed.

The Committee also received Government-confirmed evidence that the threat actor was present within Government systems for approximately 10 days before the visible attack was initiated. This 10-day undetected dwell period is central to the Committee's findings on monitoring, detection, alerting, Security Operations Centre capability, SIEM maturity, endpoint protection, privileged access management, and incident-response readiness.

The Committee accepts that independent verified sources have confirmed that personal data was compromised. The Committee also places weight on public warnings issued by the Bermuda Police Service and Government concerning phishing, scams, and actors impersonating Government after the incident. In the Committee's view, such warnings are consistent with a cyber incident involving exposure, compromise, or suspected misuse of information, and not merely a contained technical disruption.

The Committee further agrees that all available indicators suggest that a ransom demand was made and that ransom or ransom-related payment activity may have occurred. The Committee notes the Cyber Incident 2023 Budget Book line items: approximately $3.092 million under Head 10 - Ministry of Finance Headquarters, and approximately $1.323 million under Head 43 - Information and Digital Technologies, for a combined total of approximately $4.415 million. The Committee does not state, on the basis of the line items alone, that the full amount was paid as ransom. However, the scale, timing, and description of those line items require full explanation.

The Committee further considers that the $4.415 million expenditure must be assessed against the alternative scenario of rebuilding Government's affected digital environment without access to backups or original software. Based on comparable public-sector ransomware incidents and the likely scope of Government's digital environment, rebuilding without access to backups or original software could have required direct 2023 market costs in the range of $25 million to $70 million, with severe-case exposure exceeding $100 million if critical data had to be manually reconstructed or legacy systems fully replaced.

The Committee therefore recommends referral of the report and supporting materials to the Public Accounts Committee. The PAC should determine who was paid from the Cyber Incident 2023 line items, the amount and purpose of each payment, whether any payment related to ransom negotiation, decryption, data recovery, system restoration, forensic support, intermediaries, insurers, cryptocurrency facilitation, or similar activity, and whether the payment trail provides further evidence relevant to identifying parties involved in, facilitating, or benefiting from the cyber-attack.

The majority of this report is deliberately forward-looking. The Committee's principal objective is to prevent recurrence and strengthen Bermuda's national cyber resilience. The Committee recommends a dedicated National Cybersecurity Task Force, increased cybersecurity funding and specialist FTEs, a National Cybersecurity Advisory Council, a national incident response plan, a ransomware decision framework, regular independent assessments, annual cross-sector exercises, stronger backup and disaster recovery standards, Cabinet-level cyber risk oversight, improved public communications, stronger data compromise disclosure, and parliamentary implementation tracking.

The central lesson is clear: cybersecurity is no longer simply an IT function. It is critical national infrastructure.

2. Mandate, Scope, and Approach

The Joint Select Committee was established to examine the September 2023 cyber-attack affecting the Government of Bermuda and to report findings and recommendations. The Committee's work includes examining the events leading up to the attack, the adequacy of cybersecurity preparedness, the response and recovery process, the impact on Government systems and services, the status of data compromise and ransom-related matters, the expenditure associated with the incident, and the measures required to reduce the likelihood and impact of future cyber incidents.

The Committee's scope has included:

- the evolution of Government cybersecurity posture from approximately 2015 to 2025;
- the role of Information and Digital Technologies and the Chief Information Officer function;
- pre-attack warnings, including the May 2023 Cyberdine assessment;
- the implementation status of key cybersecurity controls before September 2023;
- the operational response to the September 2023 cyber-attack;
- data compromise and public scam/phishing risks;
- ransom demand and ransom-related payment indicators;
- post-incident financial allocations and expenditure;
- comparative evidence from BHB, BELCO, ABIR, and other critical-sector stakeholders; and - recommendations for a stronger cybersecurity governance, operational, and national resilience framework.

3. Methodology and Evidence Base

The Committee's work has been informed by documentary review, public record analysis, stakeholder interviews, comparative assessment, and Committee deliberation. This methodology is important because the September 2023 cyber-attack cannot be evaluated by reviewing technical systems alone. It also requires consideration of governance, funding, escalation, communications, institutional readiness, personal data protection, expenditure accountability, and public-private coordination.

3.1 Documentary Evidence The Committee reviewed materials associated with the May 2023 Cyberdine assessment, including materials showing programme status, risk level, maturity gaps, attack vectors, and recommended remediation priorities. The Committee also reviewed Government public statements during and after the attack, Budget Book extracts and line-item analysis relating to FY2023/24 cyber incident expenditure, and materials provided to the Committee.

3.2 Interviews and Stakeholder Engagement The Committee conducted interviews and engagements with Government stakeholders and external organizations. These included stakeholders connected to operational leadership, IT, cybersecurity, executive decision-making, and critical sectors such as healthcare, utilities, insurance, reinsurance, and the private sector. The purpose was to understand both the Government incident and the cyber governance practices of entities that manage critical systems and sensitive information.

3.3 Limitations and Evidentiary Approach The Committee distinguishes between established facts, strong indicators, and matters requiring further determination by the Public Accounts Committee or another competent oversight body. Where the report recommends further investigation, it does so to ensure that Parliament and the public can understand matters that were outside the Committee's direct audit or forensic mandate.

3A. Committee Use of Technical and Critical Infrastructure Evidence

The Committee's approach was to test the September 2023 cyber-attack through documentary review, witness engagement, public record analysis, critical infrastructure stakeholder evidence, and independent technical context.

The Committee was also careful to distinguish between evidence, technical interpretation, and political conclusion. The report is therefore presented as the report of the Joint Select Committee, not as the report of any one adviser, stakeholder, consultant, Department, Minister, or administration.

The Committee also considered evidence from current Government technology leadership regarding remediation steps that are now being pursued. Where current work aligns with the Committee's recommendations, the Committee welcomes that progress. The purpose of this report is not to undermine current remediation, but to ensure that such work is properly resourced, governed, documented, monitored, and sustained beyond the immediate aftermath of the incident.

4. Ten-Year Background and Cross-Administration Context

Between approximately 2015 and 2023, the Government of Bermuda became increasingly dependent on digital systems for service delivery, record management, internal communications, payroll, finance, immigration, health-related administration, public-facing transactions, and general public operations. This digital expansion improved efficiency and public access, but it also increased the consequences of cyber disruption.

The Committee considers it important to state clearly that Bermuda's 2023 cyber risk position developed over a period of years and across multiple administrations. Successive administrations led by both political parties presided over periods in which Government's digital dependency increased. During the same period, cyber threats globally became more aggressive, better organized, better funded, and more capable of disrupting public services.

The Committee does not view the September 2023 cyber-attack as the responsibility of a single Minister, Department, political party, or administration. Rather, the Committee considers that Bermuda's risk position in 2023 reflected an accumulation of structural, institutional, funding, staffing, and governance gaps that developed over time. The Committee's purpose is not to assign partisan blame, but to identify the reforms required to ensure that future administrations are not exposed to similar risks.

The evidence suggests that Government's cybersecurity governance did not consistently mature at the same pace as operational dependence on digital systems. Interviews and documentary materials suggest that cyber risk was known, but the translation of risk awareness into mature enterprise controls, clear accountability, specialist staffing, and tested recovery capability remained incomplete.

4.1 2015 to 2017: Digital Dependency Expands During the earlier part of the period under review, Government services and internal operations were already becoming more digitally dependent. Like many jurisdictions, Bermuda pursued greater use of technology for administration, communication, financial management, and public service delivery. However, digital transformation also created a wider attack surface. The Committee's concern is that cybersecurity governance and resilience planning did not develop at the same speed as reliance on digital systems.

4.2 2017 to 2022: Increasing Recognition but Incomplete Maturity Following the change in administration in 2017, Government continued to operate in an increasingly digital environment. By 2022, risk awareness had increased and Government had begun taking steps toward a more structured cybersecurity posture, including development of cybersecurity capacity and engagement of external expertise. This is an important distinction: the Committee does not find that nothing was being done. Rather, the evidence indicates that work had started but remained transitional.

The Committee finds that Government was caught between a legacy environment and a necessary future-state environment. It had identified the need for stronger cybersecurity, but had not completed the transition to mature enterprise security governance, continuous monitoring, ransomware resilience, and tested disaster recovery.

4.3 2022 to May 2023: Risk Awareness Becomes Formalized By 2022 and early 2023, the need for stronger cybersecurity had become more formalized. Government had begun engaging in assessment and remediation activity. The May 2023 Cyberdine assessment then gave the Committee a contemporaneous record of the Government's pre-attack risk posture. That assessment is central because it demonstrates that the risk was not theoretical and not merely hindsight. It was documented before the attack occurred.

4.4 Non-Partisan Institutional Lesson The Committee's non-partisan conclusion is that Bermuda's cyber risk position was shaped by years of expanding digital reliance, underinvestment or uneven investment in cybersecurity controls, specialist staffing challenges, incomplete implementation of foundational capabilities, and insufficiently mature whole-of-government cyber governance. Both political parties and multiple administrations therefore governed during stages of the accumulation of risk. The appropriate response is not partisan accusation, but structural correction.

5. How Bermuda Reached the 2023 Cyber Risk Position

The Committee identifies several structural factors that contributed to the 2023 position. These factors should be understood as cumulative rather than isolated.

Factor Relevance to 2023 position Digital dependency Government services, finance, payroll, immigration, communications, and public administration became more reliant on digital systems. Maturity gap Cybersecurity governance and operational maturity did not consistently keep pace with digital dependency. Resource constraints Specialist staffing and funding were not sufficiently aligned to the scale of cyber risk. Incomplete controls SOC/SIEM monitoring, ransomware defence, disaster recovery, backup maturity, and environment stabilization were not fully mature before the attack. Governance complexity Cybersecurity risk crossed departmental, executive, budgetary, operational, and national-security lines. Global threat escalation Ransomware groups increasingly targeted governments, healthcare, casinos, utilities, and other critical service providers.

The Committee therefore views the September 2023 attack as the foreseeable impact of a global threat environment meeting a domestic readiness gap. This does not mean the attack was inevitable. It means Bermuda must now treat cybersecurity as a standing national resilience priority, not as a project-based or incident-driven function.

6. May 2023 Cyberdine Assessment

The May 2023 Cyberdine assessment is central to the Committee's review because it provides a contemporaneous record of Government's cybersecurity posture before the September 2023 attack. The materials reviewed by the Committee indicate that Government's cyber risk was assessed as Critical. The assessment characterized this level as indicating a high probability of successful cyber-attack and limited recovery capability.

The Cyberdine materials identified root causes and structural weaknesses, including recent cyber incidents within IDT, a historical inability to deliver security initiatives and major programmes, resource constraints, lack of strategic direction, and insufficient staffing and funding. The materials also identified that Government's cybersecurity maturity was developing rather than mature.

6.1 Identified Attack Vectors The Cyberdine materials identified several attack vectors relevant to Government's environment, including phishing attacks, ransomware breach, privacy breach, cloud-based breach, and third-party risk. These risks were directly relevant to the type of incident later experienced.

6.2 Controls and Remediation Themes The materials reviewed by the Committee indicate that Government had begun a structured remediation programme. However, key capabilities were not yet fully operational or mature. These included Security Operations Centre capability, SIEM monitoring, ransomware defence, endpoint protections, disaster recovery, backup programme maturity, and broader environment stabilization.

6.3 Committee Assessment of the Cyberdine Evidence The Committee places significant weight on the May 2023 assessment because it reduces the risk of hindsight bias. It shows that material risk was known before the attack and that Government had a basis to act. The key question for the Committee is therefore not only whether Government knew of risk, but whether the response was sufficiently funded, staffed, prioritized, implemented, monitored, and escalated before the attack.

6A. Cyberdine Assessment: Receipt, Awareness, and Knowledge Transfer

The Committee places significant weight on the May 2023 Cyberdine assessment because it identified critical cyber risk before the September 2023 attack.

The Committee also considers it necessary to determine how the assessment was commissioned, who received it, who was responsible for acting on it, whether it was escalated to the appropriate senior decision-makers, and whether it was transferred effectively to subsequent technology leadership.

Evidence received by the Committee indicates that there may have been a gap in institutional awareness regarding the assessment after leadership changes. The Committee does not make a personal finding against any individual on this point. Rather, the issue is one of governance continuity: a critical cybersecurity assessment should not depend on informal memory, personality, or individual handover. It should be logged, assigned, tracked, escalated, and monitored through a formal governance process.

The Committee considers the following questions material to governance continuity:

- who commissioned the Cyberdine assessment;
- who received the assessment;
- when it was received;
- whether it was provided to the Minister, Cabinet, senior IDT leadership, or any relevant governance body;
- who was assigned responsibility for implementation;
- what remediation plan was approved;
- what funding or staffing was requested;
- what actions were completed before the attack;
- what actions remained incomplete as of 20 September 2023;
- and whether the assessment was provided to incoming or current technology leadership as part of any formal handover.

7. Implementation Gap: May to September 2023

The period between the May 2023 Cyberdine assessment and the September 2023 cyber-attack is one of the most important periods in the Committee's review. It is the period during which Government had the benefit of a formal risk assessment but had not completed implementation of several key controls.

Based on the materials reviewed, Government was in a remediation and stabilization phase. Work was underway, but important capabilities were either incomplete, not fully operational, or scheduled for later implementation. In cybersecurity, this gap matters. A known critical risk remains live until it is mitigated, accepted, transferred, or otherwise controlled through documented governance.

The Committee's concern is not that Government failed to identify risk. Rather, the concern is that identification of risk did not translate quickly enough into fully operational protective and recovery capability. The attack occurred in the interval between awareness and full readiness.

The Committee considers this implementation gap to be one of the principal lessons for future prevention. Where a critical assessment identifies high-probability/high-impact risk, Government must have an urgent remediation process, dedicated funding, named accountable officers, Cabinet-level visibility, and implementation tracking until the risk is reduced.

8. Event Reconstruction: September 2023 Cyber Attack

8.1 Initial Confirmation The public record confirms that at approximately 10:00 p.m. on Wednesday, 20 September 2023, the Bermuda Government IT system experienced a serious cyber-attack. Government stated that an immediate investigation was commenced by Information and Digital Technologies and that the matter was reported to the Bermuda Police Service.

8.2 Operational Disruption The incident affected public administration and service delivery. Government made public statements about service disruption, payroll implications, restoration work, and the staged return of services. The Committee considers that cyber incidents affecting Government must be understood as continuity-of- government incidents, particularly where payroll, public services, finance, communications, and public trust are affected.

8.3 Response and Recovery The Government's response involved containment, investigation, restoration activity, public communications, and engagement with law enforcement. The Committee accepts that recovery from a significant ransomware or cyber-extortion incident can be complex and may require external forensic support, restoration assistance, negotiation advice, legal advice, communications support, and specialist vendors. This reinforces why urgent cyber expenditure must be carefully documented and subject to later parliamentary review.

8.4 Public Communication Lessons The Committee notes the importance of public communication during and after a cyber incident. Where personal data may be compromised or misused, the public requires clear warnings, practical guidance, and confidence that Government is communicating honestly. Scam and phishing warnings are especially important where threat actors or opportunistic criminals may impersonate Government entities.

8A. Timeline of Attack, Response, and Recovery

The Committee sets out the following incident timeline based on the public record, Government evidence provided to the Committee, and evidence reviewed during its work.

May 2023 Government received the Cyberdine cybersecurity assessment. The materials reviewed by the Committee indicate that Government's cybersecurity risk posture was assessed as Critical, with a high probability of successful cyber-attack and limited recovery capability. The assessment identified risks including ransomware, phishing, privacy breach, cloud-based breach, and third-party risk.

May to September 2023 Government had begun remediation and stabilization work, but key controls were not yet fully operational or mature. These included Security Operations Centre capability, SIEM monitoring, ransomware defence, endpoint protections, disaster recovery, backup maturity, and broader environment stabilization.

Pre-Detection / Undetected Threat Actor Presence Government evidence provided to the Committee confirms that the threat actor had access to, or was present within, Government's systems for approximately 10 days before the visible attack was initiated.

This period is significant. It indicates that the September 2023 incident was not merely a single point-in-time disruption beginning when systems failed or were taken offline. Rather, the evidence shows a period of undetected presence before the operational disruption became visible.

The Committee considers this undetected period highly relevant to its findings on monitoring, detection, alerting, logging, Security Operations Centre capability, SIEM maturity, endpoint protection, privileged access management, and incident-response readiness.

The existence of a 10-day undetected dwell period reinforces the Committee's concern that Government's cyber risk posture was known to be critical before the attack, but that several foundational detection and response capabilities were not yet fully operational or mature when the incident occurred.

Wednesday, 20 September 2023 At approximately 10:00 p.m., Government's IT systems experienced the visible operational phase of the cyber-attack. Government later stated that the incident was sophisticated and deliberate. For clarity, the Committee distinguishes between the date on which the visible operational disruption occurred and the earlier 10-day period during which Government evidence confirms the threat actor was already present in the environment without detection.

Thursday, 21 September 2023 The incident was detected and Government began investigation and response activity. Information and Digital Technologies commenced work on the incident, and the matter was reported to the Bermuda Police Service. Government took systems offline as a precaution, including systems that may not have been directly affected.

September 2023 - Immediate Response Period Government services and operations were disrupted. Public reporting indicated that Government email was offline and that certain departments and public-facing services were affected. Essential services such as transport, education, and the hospital were publicly reported as continuing to operate, but basic Government systems were under significant stress.

Monday, 25 September 2023 Public reporting stated that the Premier had characterized the incident as a sophisticated and deliberate attack. It was also reported that Government expected it could take a couple of weeks for affected services to be fully restored.

Thursday, 28 September 2023 Public reporting stated that Government was slowly restoring operations. Some email functionality had returned. However, payroll and other services were still not operating normally. The Government switchboard was expected to be fully operational by the following Monday. Government also stated that it was building a stronger and more secure network with the assistance of overseas experts.

Post-September 2023 Recovery Period Government continued containment, forensic investigation, restoration, public communication, and recovery work. Further technical records will be relevant to determining the precise date on which Government considered the incident fully recovered, the date each critical system was restored, and the date any remaining temporary workarounds were retired.

FY2023/24 Budget and Expenditure Period The Budget Book recorded Cyber Incident 2023 expenditure totaling approximately $4.415 million across Head 10 - Ministry of Finance Headquarters and Head 43 - Information and Digital Technologies. The Committee recommends PAC review to determine who was paid, for what purpose, who approved the payments, and whether any payment related directly or indirectly to ransom negotiation, decryption, data recovery, system restoration, forensic support, or similar activity.

8B. Detection Expectations Based on Critical Infrastructure Stakeholder Evidence

For context, the Committee considered how the Government-confirmed 10-day undetected presence period compares with the cybersecurity practices described by critical infrastructure stakeholders who provided evidence, submissions, or engagement to the Committee.

The Committee does not adopt a single universal "industry standard" detection period. The evidence received indicates that detection capability depends on the maturity of an organization's logging, endpoint detection and response, identity monitoring, Security Operations Centre coverage, SIEM capability, privileged access controls, threat hunting, incident escalation, and whether the attacker uses malware, stolen credentials, or legitimate administrative tools.

However, evidence from critical infrastructure stakeholders assisted the Committee in identifying the features of a mature monitored environment. Such an environment would generally include continuous or near-continuous security monitoring, alert triage, endpoint visibility, privileged-access monitoring, tested escalation procedures, backup integrity checks, and clear incident-response governance.

In that type of mature monitored environment, high-risk malicious activity would generally be expected to generate alerts within hours or days, particularly where activity involves unusual access patterns, lateral movement, privilege escalation, mass file activity, attempted backup interference, data staging, or encryption preparation. The Committee accepts that not every intrusion can be detected immediately, especially where an attacker uses legitimate credentials or "living off the land" techniques. Nevertheless, a 10-day undetected presence before the visible attack phase is materially significant when compared with the level of monitoring and escalation expected in a mature critical-infrastructure environment.

Accordingly, the more important comparison is not simply the date on which Government systems became visibly disrupted. The more important governance question is how long the threat actor was present before detection, and whether Government had the monitoring, alerting, logging, and response capability to identify reconnaissance, credential misuse, lateral movement, privilege escalation, data access, data staging, or backup tampering before the attack was initiated.

The Government-confirmed dwell period of approximately 10 days is significant. It shows that the actor was able to operate inside the environment before the incident became visible. That fact is directly relevant to the Committee's findings regarding SOC/SIEM maturity, endpoint detection and response, identity and privileged-access monitoring, logging retention, threat hunting, and incident-response readiness.

The Committee therefore considers the critical infrastructure stakeholder evidence to be important not because Government should be identical to any one private-sector or statutory body, but because those stakeholders manage essential services, sensitive information, operational continuity risk, public confidence, and reputational exposure. Their evidence provides a practical benchmark for the minimum level of cyber visibility, monitoring, escalation, and resilience that should be expected across Government systems.

This comparison reinforces the Committee's concern that Government's cyber risk posture was known to be critical before the attack, but that foundational detection and response capabilities were not sufficiently mature at the time of the September 2023 incident.

This comparison is central to prevention. It shows that the September 2023 incident should not be assessed only by when Government systems went offline, but by whether Government had the capability to detect and disrupt the actor before the visible attack was launched.

9. Data Compromise and Public Risk

The Committee accepts that independent verified sources confirm that personal data was compromised. The final evidence bundle should identify the source or sources relied upon, the nature of the confirmation, the categories of data implicated where known, and the appropriate level of public or confidential disclosure.

The Committee also notes that the Bermuda Police Service and Government issued public warnings concerning phishing, scams, and actors impersonating Government. Those warnings are relevant because they indicate that members of the public faced downstream risks associated with exposed, compromised, or misused information. In the Committee's view, such warnings are consistent with a cyber incident involving data compromise or the credible risk of misuse of Government-related information.

The Committee recommends that Government establish a clear future process for assessing, confirming, and disclosing data compromise. This process should include forensic assessment, notification to the Privacy Commissioner where required, identification of affected data categories, risk assessment for affected persons, public guidance, direct notification where appropriate, identity-protection advice, and post-incident reporting to Cabinet and Parliament.

10. Ransom Indicators and Cyber Incident 2023 Expenditure

The Committee agrees that all available indicators suggest that a ransom demand was made and that a ransom or ransom-related payment may have been effected. The Committee's view is based on the nature of ransomware operations generally, the modus operandi of ALPHV/BlackCat-type incidents, the existence of Cyber Incident 2023 expenditure, and the unresolved need for a transparent payment trail.

The Committee is careful not to overstate the current public record. The Budget Book line items do not, by themselves, prove that the full amount was paid to a threat actor. They do, however, confirm significant public expenditure connected to the cyber incident and require a full explanation.

Head / Department Business Unit Description Amount Head 10 - Ministry of Finance 20996 Cyber Incident 2023 $3.092 million Headquarters Head 43 - Information and 53996 Cyber Incident 2023 $1.323 million Digital Technologies Combined - Cyber Incident 2023 line items Approx. $4.415 million The Committee considers that the scale, timing, and description of these allocations require examination by the Public Accounts Committee. The central questions are who received the payments, what each payment was for, who approved each payment, whether any payment related to ransom negotiation or recovery assistance, and whether the payment trail provides further evidence relevant to identifying parties involved in, facilitating, or benefiting from the attack.

10A. Recovery, Rebuilding Without Access to Backups or Original Software, and the Public Value Question The Committee considers it necessary to distinguish between three related but different concepts:

- Emergency restoration of Government services;

- Recovery and stabilization of affected systems;

- Rebuilding Government's digital environment without access to backups or original software.

The public record confirms that the cyber-attack occurred late on Wednesday, 20 September 2023, and that Government was still restoring operations more than one week later. Public reporting stated that some email functionality had returned by 28 September 2023, but that payroll and other services were still not operating normally. It was also publicly reported that Government had taken all systems offline as a precaution and was building a more secure network with assistance from overseas experts.

The Committee accepts that, in a major cyber incident, emergency restoration may be faster than rebuilding without access to backups or original software. Recovery with the assistance of external specialists can allow Government to restore priority services, preserve institutional data, rebuild trust in selected systems, and resume operations in stages.

Rebuilding without access to backups or original software, by contrast, may require new architecture, emergency procurement, system reconfiguration, identity redesign, security controls,

testing, user onboarding, data validation, legacy-system replacement, staff training, and continuity planning across Ministries and Departments.

The Budget Book line items reviewed by the Committee record approximately $3.092 million under Head 10 - Ministry of Finance Headquarters and approximately $1.323 million under Head 43 - Information and Digital Technologies, for a combined total of approximately $4.415 million connected to Cyber Incident 2023 expenditure.

The Committee does not state, on the present evidence, that the full $4.415 million was paid as ransom. Nor does the Committee state, without further evidence, that the sum represents the total cost of recovery. However, the scale and timing of this expenditure raise an important public value question: did the payments made from the Cyber Incident 2023 line items allow Government to recover faster and at lower overall public cost than rebuilding the affected environment without access to backups or original software would have required?

The Committee considered what the likely cost and operational impact would have been if Government had been required to rebuild its affected digital environment without access to usable backups, trusted original software, clean system images, identity configuration, application deployment files, reliable recovery tooling, or validated system documentation.

The Committee cannot responsibly state a precise rebuild cost without verified evidence from IDT, vendors, procurement records, and the Public Accounts Committee. However, based on comparable public-sector ransomware incidents and the likely scope of Government's digital environment, the Committee considers it reasonable to conclude that rebuilding without access to backups or original software could have required direct 2023 market costs in the range of $25 million to $70 million, with severe-case exposure exceeding $100 million if critical data had to be manually reconstructed or legacy systems fully replaced.

The operational impact would also likely have been substantial. Government may have been able to establish manual or temporary workarounds within days or weeks for selected essential services. However, without usable backups or original software, the Committee considers it likely that Government would have faced several months of severe operational impairment, six to twelve months of materially degraded digital services, and twelve to twenty-four months before full functional recovery, audit confidence, data validation, and security hardening were achieved.

The Committee's assessment is therefore that rebuilding without access to backups or original software would likely have taken substantially longer than the staged restoration achieved after the incident. Such a rebuild may have required many months, and potentially more than one financial year, depending on the number of systems affected, the state of backups, the integrity of identity infrastructure, procurement requirements, available specialist staffing, the availability of original software or vendor deployment packages, and the need to validate, reconstruct, or migrate data.

This comparison is important when considering the Cyber Incident 2023 expenditure totaling approximately $4.415 million. The Committee does not state that the full amount was paid as ransom, nor that the expenditure represented the total cost of recovery. However, the expenditure should be assessed against the alternative scenario of prolonged outage, digital service failure,

system reconstruction, data reconstruction, emergency procurement, and extended disruption to public services.

The public should understand not only how much was spent, but what was achieved by that expenditure. If the expenditure helped Government avoid a longer, more disruptive, and more expensive rebuilding process, that should be clearly explained. If the expenditure did not produce that value, or if any portion related to ransom or ransom-related activity, that must also be transparently reviewed.

Accordingly, the Committee recommends that the Public Accounts Committee, or another competent oversight body, require Government to provide a formal recovery-versus-rebuild analysis, including:

- the systems affected by the cyber-attack;

- the date each critical system was restored;

- the date Government considered the incident fully recovered;

- the vendors, firms, intermediaries, or other recipients paid from the Cyber Incident 2023 line items;

- the purpose of each payment;

- whether any payment related to ransom negotiation, decryption, data recovery, system restoration, forensic support, legal advice, communications support, cryptocurrency facilitation, insurance, or similar activity;

- the estimated time and cost of rebuilding the affected environment without access to backups or original software;

- the estimated time saved by using external recovery support;

- the estimated cost avoided by not having to rebuild without access to backups or original software;

- and whether the expenditure represented value for money when compared with the likely cost, delay, and operational disruption of such a rebuild.

The Committee therefore recommends that any public account of the incident include a recovery timeline, a payment trail, and a comparator showing the likely cost, duration, and operational impact of rebuilding Government's affected digital environment without access to backups or original software.

11. Governance, Accountability, and Non-Partisan Findings

Governance and accountability are central to understanding the causes and consequences of the September 2023 attack. The incident cannot be adequately explained only by reference to malware, threat actors, or technical compromise. It must also be understood through decision-making, escalation, funding, workforce capability, executive ownership, risk reporting, and implementation of previously identified controls.

Operational responsibility for Government IT systems sat within the relevant technical functions. However, cybersecurity risk is enterprise-wide. Where risk is critical, accountability cannot sit only at the technical level. It must be visible to senior officials, Ministers, Cabinet, and, where appropriate, Parliament.

The Committee's non-partisan finding is that successive administrations contributed to the context in which Bermuda arrived at the 2023 position. This is not a finding of equal fault or identical conduct. It is a finding that the risk accumulated over time while digital reliance increased under multiple governments. The appropriate remedy is not partisan blame, but durable institutional reform capable of protecting Bermuda regardless of which party forms Government.

The Committee therefore recommends that future cybersecurity governance be structured so that critical risks cannot be known but remain insufficiently visible, insufficiently funded, or insufficiently implemented.

12. Comparative Case Studies: ALPHV/BlackCat and Similar Ransomware Attacks

The Committee includes comparative case studies to demonstrate that Bermuda's September 2023 incident occurred during a wider period of ransomware and cyber-extortion activity affecting governments, casinos, healthcare systems, and critical service providers. These cases are not included to prove identical facts in Bermuda. They are included to support lessons on data compromise, ransom governance, critical- service disruption, public communication, recovery planning, and payment-trail accountability.

12.1 ALPHV/BlackCat Operating Pattern ALPHV/BlackCat has been publicly described as a ransomware-as-a-service operation. Public reporting and law-enforcement-related reporting describe a model involving affiliates, extortion, encryption, data theft or data-leak pressure, and ransom demands. The relevance to Bermuda is that modern ransomware incidents commonly involve both operational disruption and threatened or actual data compromise. Payment may be sought not only for decryption, but also for promises relating to deletion, non- publication, or recovery support.

A December 2023 U.S. law-enforcement operation disrupted ALPHV/BlackCat infrastructure and involved a decryption tool made available to victims who contacted law enforcement. That event is relevant because it occurred shortly after the Bermuda incident and highlights the international seriousness of the ransomware threat environment in which Bermuda was operating.

12.2 MGM Resorts and Caesars Entertainment - September 2023 In September 2023, MGM Resorts and Caesars Entertainment suffered major cyber incidents around the same period as the Bermuda attack. Public reporting connected the activity to Scattered Spider and ALPHV/BlackCat-related actors. MGM experienced substantial operational disruption, including impacts to hotels, reservations, and casino operations. MGM later disclosed an approximate $100 million impact to third-quarter results. Public reporting indicated that Caesars experienced a social-engineering attack involving an outsourced IT support vendor and that customer personal information, including driver's license and Social Security information for a significant number of loyalty programme members, was compromised.

The MGM/Caesars comparison is important for Bermuda for four reasons. First, it shows that social engineering and identity-based compromise can defeat organizations that otherwise appear sophisticated. Second, it shows that operational disruption can affect public confidence quickly. Third, it shows that personal information can become central to extortion pressure. Fourth, it shows why payment and non- payment decisions require a pre-existing governance framework, because the consequences of either decision are serious.

12.3 Change Healthcare / UnitedHealth Group - 2024 The Change Healthcare incident is relevant because it involved ALPHV/BlackCat attribution, disruption to a critical healthcare payments network, public consequences for patients, pharmacies, and healthcare providers, and reporting concerning a $22 million ransom-related payment. The incident illustrates that ransomware can affect essential services far beyond the initially targeted system and that recovery may involve enormous operational, financial, and public-trust consequences.

For Bermuda, the lesson is that cyber resilience cannot be treated as a back-office IT issue. If Government systems, healthcare systems, financial services systems, utilities, telecommunications, airport operations, or public payment functions are compromised, the consequences may quickly become national in scope.

12.4 Lessons for Bermuda The comparative case studies support the following lessons for Bermuda:

- Data risk: Modern ransomware incidents often involve data theft, not only encryption. Bermuda must have a data compromise assessment and disclosure process.

- Ransom governance: Ransom demands must be handled through a pre-approved framework with law enforcement, Cabinet oversight, legal advice, and financial audit trails.

- Operational continuity: Cyber incidents can disrupt essential services. Recovery planning and tested backups are core public-service obligations.

- Social engineering: MFA alone is insufficient if help desks, vendors, privileged access, and identity workflows are vulnerable.

- Payment accountability: Payments to vendors, negotiators, intermediaries, or recovery providers must be documented and reviewable after the incident.

- Public communication: Public warnings must be timely and specific when phishing, scams, impersonation, or identity misuse risks arise.

13. Key Findings

The Committee makes the following key findings:

1. **Government became increasingly digitally dependent over the years leading to 2023. Digital reliance increased across public services, finance, communications, and operations.**

2. **The 2023 risk position was cross-administration and non-partisan. Successive administrations led by both political parties governed during the accumulation of cyber risk.**

3. **Government was on notice of critical cybersecurity risk before the attack. The May 2023 Cyberdine assessment identified a Critical cyber risk posture.**

4. **The attack occurred during an implementation gap. Risk awareness existed, but key controls were not fully operational or mature before the attack.**

5. **Personal data was compromised. The Committee relies on independent verified sources and post-incident scam/phishing warnings in reaching this conclusion.**

6. **All available indicators suggest that a ransom demand and ransom-related payment activity may have occurred. The Committee's view is based on ransomware modus operandi, comparative cases, line-item expenditure, and the unresolved public record.**

7. **Cyber Incident 2023 expenditure requires full review. The approximately $4.415 million in line items requires explanation of recipients, purposes, approvals, and payment trails.**

8. **Prevention requires national resilience reform, including a Task Force, advisory council, funding, FTEs, incident plan, ransomware framework, exercises, and parliamentary oversight.**

14. Committee Conclusion

The Committee concludes that the September 2023 cyber-attack occurred in a known risk environment. Government had been warned of a Critical cybersecurity posture in May 2023. Remediation had begun, but key controls were incomplete or not fully operational when the attack occurred.

The Committee further concludes that the incident exposed weaknesses not only in technical controls, but also in governance, implementation discipline, resource allocation, workforce capacity, data compromise disclosure, public communication, and financial accountability.

The Committee agrees that all available indicators suggest that personal data was compromised and that a ransom demand and ransom-related payment activity may have occurred. The Committee is of the view that the Cyber Incident 2023 line items totaling approximately $4.415 million require full Public Accounts Committee review to determine who was paid, for what purpose, and whether the payment trail provides further clarity regarding ransom-related activity, system recovery, data recovery, or parties involved in, facilitating, or benefiting from the attack.

The Committee's most important conclusion, however, is forward-looking: Bermuda must build a national cyber resilience framework capable of protecting critical public services, personal data, and public confidence regardless of which administration is in office.

15. Recommendations for Prevention and National Cyber Resilience

The following recommendations are intentionally prevention-focused. The Committee's view is that the most important question for Parliament is what Bermuda must now build so that a similar incident is less likely to occur and, if it does occur, the national response is faster, better governed, and more transparent.

15.1 Treat cybersecurity as critical national infrastructure Government should formally treat cybersecurity as critical national infrastructure. It is central to continuity of Government, public confidence, data protection, national security, financial services, healthcare, utilities, ports, airport operations, and Bermuda's international reputation.

15.2 Establish a dedicated National Cybersecurity Task Force Government should establish a standing National Cybersecurity Task Force with defined authority, reporting lines, and responsibility for preparedness, threat monitoring, incident response coordination, and post-incident recovery. The Task Force should work directly with IDT, BPS, Cabinet Office, National Security, Attorney-General's Chambers, the Privacy Commissioner, and critical infrastructure stakeholders.

15.3 Increase dedicated cybersecurity funding Government should create a dedicated and recurring cybersecurity budget line separate from general IT expenditure. Funding should support threat monitoring, SOC/SIEM/EDR capability, vulnerability management, penetration testing, ransomware resilience, backup maturity, cloud security, identity and access management, training, and incident-response retainers.

15.4 Increase Government cybersecurity FTEs Government should increase full-time equivalent cybersecurity positions. Cybersecurity should not be treated as an additional duty of general IT staff. Specialist roles are required in governance, threat intelligence, incident response, digital forensics, security architecture, cloud security, vulnerability management, privacy, disaster recovery, and policy compliance.

15.5 Create a National Cybersecurity Advisory Council Government should establish a National Cybersecurity Advisory Council comprising senior cyber, technology-risk, and security professionals from critical sectors, including but not limited to BELCO, ABIC, ABIR, BHB, Butterfield, HSBC, telecommunications providers, airport and port stakeholders, and other critical infrastructure or regulated-sector organizations. The Council should meet quarterly and be available to advise Cabinet and the Task Force during a major cyber incident.

15.6 Develop a National Cyber Incident Response Plan Government should approve and test a National Cyber Incident Response Plan identifying who leads during an incident, when Cabinet is briefed, when law enforcement is engaged, who communicates with the public, how critical services are prioritized, how ransom demands are handled, how personal-data compromise is assessed, and when Parliament is updated.

15.7 Establish a formal ransomware decision framework Government should adopt a ransomware decision framework covering whether Government will negotiate, who can approve any negotiation or payment-related decision, how law enforcement and insurers are involved, how cryptocurrency

or intermediaries are handled, how approvals are documented, and how Parliament and PAC are notified after the fact.

15.8 Strengthen backup, disaster recovery, and business continuity Government should implement minimum resilience standards for all Ministries and Departments, including tested offline backups, immutable backup capability where appropriate, recovery-time objectives, recovery-point objectives, annual testing, independent backup verification, and priority restoration plans for essential services.

15.9 Require regular independent cybersecurity assessments Government should commission regular independent cybersecurity assessments, including maturity reviews, penetration testing, vulnerability assessments, ransomware readiness assessments, cloud- security reviews, identity and access-management reviews, third-party risk reviews, and implementation audits of prior recommendations.

15.10 Require formal remediation plans for critical findings Where an independent assessment identifies critical risk, Government should prepare a remediation plan with responsible officers, timelines, funding, milestones, and Cabinet-level oversight until the risk is mitigated or formally accepted.

15.11 Strengthen public communication and scam warnings Government should establish a public communications protocol for phishing, impersonation, identity theft, fake Government communications, and fraudulent payment demands. Public warnings should be timely, coordinated, clear, and accessible.

15.12 Improve data compromise assessment and disclosure Government should establish a clear process for determining whether personal data has been compromised, including forensic assessment, Privacy Commissioner notification, categorization of affected data, public communication, direct notification where appropriate, and identity-protection guidance.

15.13 Require Cabinet-level cyber risk oversight Cabinet should receive scheduled cybersecurity briefings at least quarterly, covering threat environment, maturity, critical risks, remediation progress, funding, staffing gaps, readiness, and critical infrastructure dependencies.

15.14 Conduct annual cross-sector cyber exercises Government should conduct annual cyber exercises involving Government, BPS, BHB, BELCO, major banks, insurers, telecommunications providers, airport and port stakeholders, emergency services, relevant regulators, and Cabinet-level observers.

15.15 Develop a critical infrastructure cybersecurity framework Bermuda should develop a critical infrastructure cybersecurity framework covering Government digital services, healthcare, energy, telecommunications, banking and payments, insurance and reinsurance, airport and ports, water and waste systems, and emergency services.

15.16 Strengthen third-party and vendor risk management Government should strengthen procurement and contract requirements for vendors with access to Government systems or data,

including minimum cyber standards, incident reporting, cyber insurance where appropriate, and mandatory cooperation during incidents.

15.17 Strengthen identity, access, and privileged account controls Government should prioritize multi-factor authentication, privileged access management, least-privilege access, account lifecycle management, conditional access, and monitoring of privileged accounts.

15.18 Establish continuous security monitoring Government should ensure continuous security monitoring through SOC/SIEM/EDR capability, threat intelligence, alert triage, and escalation procedures. Where 24/7 in-house capability is not immediately possible, Government should consider a managed security service with strong oversight.

15.19 Require mandatory cyber training and phishing simulations Government should require regular cybersecurity awareness training and phishing simulations for public officers, with enhanced role-based training for senior leaders, finance officers, system administrators, communications staff, and persons handling sensitive personal data.

15.20 Improve data classification and retention Government should implement a data classification and retention framework so sensitive data is identified, access-controlled, encrypted where appropriate, and not retained longer than necessary.

15.21 Establish an emergency cyber expenditure protocol Government should establish a protocol for urgent cyber expenditure, including approval thresholds, Cabinet notification, documentation requirements, vendor justification, payment records, and post- incident review.

15.22 Improve parliamentary oversight and implementation tracking Government should report periodically to Parliament on cyber readiness while protecting sensitive operational details. Accepted recommendations should be placed in an implementation tracker identifying responsible departments, timelines, funding status, and progress.

15.23 Require mandatory post-incident review Any major cyber incident affecting Government systems should trigger a mandatory post-incident review addressing cause, systems affected, data compromise, response timeline, public communications, expenditure, ransom demands or payments, recovery actions, accountability, and reforms required.

15.24 Proposed National Cyber Resilience Operating Model The Committee recommends that Government move from an ad hoc cyber response model to a standing national cyber resilience operating model. The model should identify standing responsibilities before an incident, escalation responsibilities during an incident, and accountability responsibilities after an incident.

The operating model should include the following responsibilities:

- Cabinet: Receive quarterly cyber risk briefings, approve funding priorities, receive urgent incident briefings, approve extraordinary decisions, and ensure whole-of-government coordination.

- National Cybersecurity Task Force: Coordinate preparedness, threat monitoring, exercises, response plans, remediation tracking, and operational response across Government, law enforcement, regulators, communications, and critical sectors.

- IDT / Technical Lead: Maintain systems, monitoring, backups, identity controls, vulnerability management, and remediation plans; lead technical containment, restoration, forensic engagement, and operational recovery.

- Bermuda Police Service: Maintain cybercrime liaison, evidence handling protocols, and public scam-warning capability; support criminal investigation, preservation of evidence, international law-enforcement liaison, and scam warnings.

- Privacy Commissioner / Data Protection Functions: Maintain data breach reporting expectations and privacy guidance; advise on data compromise assessment, notification obligations, and risk to affected persons.

- National Cybersecurity Advisory Council: Meet quarterly to share sector risk, readiness, dependency mapping, and best practice; provide strategic advice to Cabinet and the Task Force during major incidents.

- Parliament / PAC: Receive periodic readiness reporting and implementation updates; conduct post-incident expenditure and accountability review where public funds are used.

15.25 National Cybersecurity Task Force - Minimum Terms of Reference The Committee recommends that the National Cybersecurity Task Force be established with written terms of reference. At a minimum, those terms should include:

- maintaining the National Cyber Incident Response Plan;

- maintaining a national cyber risk register for Government and critical public services;

- tracking implementation of critical and high-risk remediation items;

- coordinating annual tabletop exercises and after-action reviews;

- maintaining incident escalation protocols for Cabinet and senior officials;

- maintaining relationships with law enforcement, regulators, private-sector cyber leaders, and international cyber partners;

-ensuring that ransomware decision-making, data compromise assessment, public communications, and emergency expenditure protocols are tested before an incident occurs;

- submitting quarterly cyber readiness reports to Cabinet and annual summaries to Parliament, subject to necessary security redactions.

15.26 National Cybersecurity Advisory Council - Role and Composition The Committee recommends that the National Cybersecurity Advisory Council be advisory, not operational. It

should not replace Government accountability or private-sector responsibility. Its purpose should be to ensure that Bermuda's most cyber-mature sectors can share practical intelligence, identify cross-sector dependencies, and advise Cabinet during a major event.

The Council should include representation or input from:

- BELCO / energy sector, because energy disruption can have island-wide consequences and cyber resilience is critical to continuity.

- BHB / healthcare, because healthcare systems hold sensitive data and support essential public services.

- ABIC / international business, because international business depends on Bermuda's reputation for operational and regulatory resilience.

- ABIR / insurance and reinsurance, because insurance/reinsurance stakeholders understand cyber risk, claims, modelling, and international expectations.

- Major banks including Butterfield and HSBC, because banking and payments infrastructure are critical to daily life, confidence, and recovery.

- Telecommunications providers, because connectivity is essential during incident response and recovery.

- Airport, ports, and critical transport stakeholders, because transport disruption can affect movement, supply chains, tourism, and emergency response.

- Privacy and legal expertise, because data compromise, notification, privilege, evidence handling, and public communication require legal discipline.

The Council should meet quarterly in normal conditions. During a major cyber incident, it should be capable of convening rapidly to provide Cabinet-level advice on cross-sector impacts, public communication, business continuity, and recovery priorities.

15.27 Minimum Cyber Control Baseline The Committee recommends that Government establish a minimum cyber control baseline for all Ministries, Departments, and critical public systems. This baseline should be measurable and audited periodically.

At minimum, the baseline should include:

- Identity and access: MFA, least privilege, privileged access management, account lifecycle controls, and monitoring of privileged accounts.

- Endpoint and server protection: Endpoint detection and response, patching standards, malware protection, and security configuration baselines.

- Security monitoring: SOC/SIEM capability, alert triage, threat intelligence, and documented escalation procedures.

- Backup and recovery: Offline or immutable backups where appropriate, tested restoration, recovery-time objectives, recovery-point objectives, and backup integrity verification.

- Vulnerability management: Regular scanning, risk-based remediation timelines, penetration testing, and executive reporting of overdue critical findings.

- Cloud and third-party risk: Vendor cyber standards, access controls, contractual incident reporting, and cloud configuration review.

- Data protection: Data classification, encryption where appropriate, retention limits, breach assessment, and disclosure procedures.

- Training and culture: Mandatory awareness training, phishing simulations, role-based training, and senior-leader cyber briefings.

15.28 Funding and Workforce Model The Committee recommends that Government move away from episodic cyber funding and adopt a recurring funding and workforce model. Cybersecurity cannot be adequately funded only after an incident has occurred. It requires predictable investment, specialist roles, training, tools, retainers, and continuous improvement.

Government should prepare a cybersecurity workforce plan identifying current cyber-related posts, vacancies, required future FTEs, priority specialist roles, training needs, succession risks, and whether managed services are required while internal capacity is built.

Funding and workforce priorities should include:

- Dedicated cyber budget line, to separate cybersecurity from general IT operations and allow Parliament to track investment.

- Incident response retainer, to ensure rapid access to forensic, legal, communications, and recovery support.

- SOC/SIEM/EDR funding, to support monitoring, detection, and response capability.

- Training and certification, to build internal competence and reduce dependence on a small number of individuals.

- Cyber policy and compliance capacity, to ensure assessments lead to implementation, not merely reports.

- Digital forensics and investigation support, to improve evidence handling and law-enforcement coordination.

15.29 Public Communication and Trust Protocol The Committee recommends that Government adopt a public communication protocol designed to maintain trust while avoiding premature or unsupported technical claims. The protocol should require Government to communicate what is known, what is not yet known, what the public should do, what services are affected, when the next

update will be provided, and what specific scam, phishing, or impersonation risks the public should watch for.

Where personal data may be compromised, communications should be coordinated with privacy, legal, technical, and law-enforcement advice. The public should receive practical guidance such as not clicking suspicious links, verifying Government communications through official channels, monitoring accounts, and reporting suspicious messages.

15.30 Recommended Cyber Readiness Dashboard The Committee recommends that Cabinet and appropriate oversight bodies receive a recurring cyber readiness dashboard. Sensitive technical details may be redacted for broader circulation, but decision-makers should receive enough information to understand risk and progress.

The dashboard should track:

- Critical risks open, to show whether severe risks remain unresolved.

- Remediation progress, to show whether recommendations and assessment findings are being implemented.

- Backup test status, to show whether Government can recover essential systems.

- Incident response exercise status, to show whether plans are being tested.

- Cyber FTE vacancies, to show workforce risk.

- Training completion rates, to show cyber culture and readiness.

- Vendor risk status, to show third-party exposure.

- Budget status, to show whether cyber priorities are funded.

15.31 Accountability for Implementation The Committee recommends that each accepted recommendation be assigned to a named lead Ministry, Department, or office. Each recommendation should have a target date, funding status, implementation status, and reporting requirement. Without implementation tracking, cyber reports risk becoming another unfulfilled document rather than a programme of reform.

15A. Public Protection Checklist During Cyber Incidents

The Committee considers that future cyber incident response planning should include a clear public protection checklist.

In the same way that Government provides hurricane-preparedness guidance, Government should be able to issue practical cyber-protection instructions during or after a major cyber incident. Such guidance should be prepared in advance and issued quickly when personal data exposure, phishing, impersonation, identity theft, or scam risk is suspected.

The checklist should include clear public instructions such as:

- change passwords for Government-facing accounts where applicable;

- change passwords for any private accounts where the same password may have been reused;

- enable multi-factor authentication wherever possible;

- monitor banking, email, and online accounts for suspicious activity;

- verify Government messages through official channels;

- do not click suspicious links or payment requests;

- report impersonation attempts, phishing messages, and suspicious calls;

- preserve suspicious messages as evidence where appropriate;

- and follow updates from designated official communication channels.

The Committee does not suggest that every incident will require the same public warning. However, where there is credible risk of personal data misuse, Government should not merely state that systems are being restored. It should tell the public what practical steps they should take to protect themselves.

15B. From Incident Response to Standing Cyber Readiness

The Committee's review reinforces that cybersecurity cannot be treated as a project that becomes urgent only after an attack. It must be treated as a standing readiness function.

The Committee therefore links the September 2023 incident directly to its recommendations for a National Cybersecurity Task Force, Cabinet-level cyber risk oversight, increased cybersecurity FTEs, and a dedicated function or capability capable of monitoring cyber risk on a continuous or near-continuous basis.

The purpose of these recommendations is not only to respond better after a future incident, but to detect, escalate, and disrupt malicious activity before an incident reaches the visible disruptive stage.

16. Recommendation for Referral to the Public Accounts Committee

The Committee recommends that this report, together with the relevant supporting materials, be referred to the Public Accounts Committee for further consideration.

In particular, the Committee recommends that the Public Accounts Committee examine the expenditure recorded under the Cyber Incident 2023 Budget Book line items totaling approximately $4.415 million.

The purpose of that referral should be to determine:

- who was paid from those line items;

- the amount paid to each recipient;

- the purpose and justification for each payment;

- whether any payments were made to cyber-response firms, forensic firms, negotiators, insurers, intermediaries, cryptocurrency facilitators, or other third parties;

- whether any payment was made directly or indirectly in connection with a ransom demand, ransom negotiation, decryption assistance, system restoration, data recovery, or data-deletion assurance;

- whether the payment trail provides further evidence relevant to identifying parties involved in, facilitating, or benefiting from the September 2023 cyber attack; and - whether any further referral to law enforcement, audit, or other competent authorities is required.

The Committee considers this referral necessary because the existing Budget Book line items confirm significant public expenditure connected to the cyber incident, but do not, on their face, provide sufficient transparency as to ultimate recipients, purpose, approvals, or nature of the payments.

16A. No Finding of Impropriety, but Need for Financial Review

The Committee reviewed evidence indicating that approximately $4.415 million was expended on response, recovery, restoration, consultation services, and related cybersecurity activities following the September 2023 cyber-attack.

The Committee did not conduct a detailed financial audit, procurement compliance review, or payment-trail investigation. The Committee therefore makes no finding of impropriety in relation to this expenditure.

However, the Committee considers that the scale, timing, and description of the expenditure require further examination by the appropriate parliamentary oversight body. The central issue is not whether money was spent - it plainly was. The central issue is whether Parliament and the public can determine who was paid, what services were provided, what approvals were obtained, whether procurement and emergency contracting controls were followed, whether value for money was

achieved, and whether any payment related directly or indirectly to ransom negotiation, decryption, data recovery, system restoration, or similar activity.

Accordingly, the Committee recommends that the Public Accounts Committee, or another competent oversight body, conduct a further review of the Cyber Incident 2023 expenditure.

17. Implementation Roadmap

The Committee recommends a staged implementation roadmap:

0-90 days:

- Refer expenditure to PAC;

- preserve all incident financial records;

- confirm data compromise disclosure status;

- establish an interim Task Force;

- begin Cabinet cyber risk briefings;

- identify urgent funding and FTE needs.

3-6 months:

- Complete workforce gap analysis;

- convene the National Cybersecurity Advisory Council;

- approve an interim ransomware decision framework;

- commission an independent assessment;

- produce a remediation tracker.

6-12 months:

- Approve the National Cyber Incident Response Plan;

- conduct the first national tabletop exercise;

- implement priority SOC/SIEM/EDR improvements;

- test backup and disaster recovery for essential services.

12-24 months:

- Operationalize the cyber FTE plan;

- mature the advisory council and exercises;

- implement the critical infrastructure cyber framework;

- strengthen vendor risk standards;

- report progress to Parliament.

18. Final Conclusion

The September 2023 cyber attack exposed a national resilience gap. The Committee's view is that the appropriate response is not only to determine what happened, but to ensure that Bermuda builds the structures, funding, staffing, oversight, and public-private coordination needed to prevent recurrence and respond effectively to future incidents.

The Committee agrees that all available indicators suggest that personal data was compromised and that a ransom demand and ransom-related payment activity may have occurred. The Cyber Incident 2023 line items totaling approximately $4.415 million require full Public Accounts Committee review to determine who was paid, for what purpose, and whether the payment trail provides further evidence relevant to the attack.

Most importantly, the Committee concludes that cybersecurity must be treated as critical national infrastructure. The reforms recommended in this report are directed toward prevention, resilience, accountability, and the protection of the public. They are also designed to ensure that future governments, regardless of political party, inherit a stronger and more resilient cybersecurity framework than existed in September 2023.

Signature Page

Report of the Joint Select Committee on the September 2023 Cyber Attack on the Government of Bermuda Submitted to the Honourable House of Assembly We, the undersigned Members of the Joint Select Committee, submit this report for the consideration of the House.

Lawrence Scott, JP, MP Chair Joint Select Committee

Date: 13 July 2026

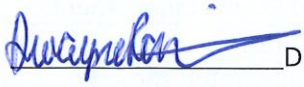
Scott Simmons, JP, MP Member Joint Select Committee

Date: 13 July 2026

Jamahl S. Simmons, JP, MP Member Joint Select Committee

Date: July 10, 2026

Dwayne Robinson, JP, MP Member Joint Select Committee



Date: July 10, 2026

Appendix A. Glossary of Acronyms and Key Terms

This glossary is provided to assist readers with acronyms and recurring technical or institutional terms used in the report.

Acronym / Term	Meaning
ABIC	Association of Bermuda International Companies.
ABIR	Association of Bermuda Insurers and Reinsurers.
ALPHV/BlackCat	Ransomware-as-a-service operation referenced in the comparative case studies.
BELCO	Bermuda Electric Light Company.
BHB	Bermuda Hospitals Board.
BPS	Bermuda Police Service.
Cyberdine	Cybersecurity firm whose May 2023 assessment is referenced in the report.
EDR	Endpoint Detection and Response.
FTE / FTEs	Full-Time Equivalent / Full-Time Equivalents.
FY2023/24	Financial Year 2023/24.
HSBC	HSBC Bank Bermuda Limited; referenced as a major banking stakeholder.
IDT	Information and Digital Technologies.
IT	Information Technology.
JP	Justice of the Peace.
JSC	Joint Select Committee.
MFA	Multi-Factor Authentication.
MGM	MGM Resorts; referenced in the comparative cyber incident case studies.
MP	Member of Parliament.
PAC	Public Accounts Committee.
SIEM	Security Information and Event Management.
SOC	Security Operations Centre.
SOC/SIEM/EDR	Shorthand reference to integrated security monitoring, event management, and endpoint detection and response capability.