RESEARCH REPORT

The Five Cyber Investments That Deliver Disproportionate Risk Reduction.

Not all security spending is equal. This analysis identifies the five areas where the gap between investment and risk reduction is largest, and where underspending is most dangerous for mid-market and public sector organisations.

2026	$5M+	5
Research Cycle	**Organisation Range**	**Priority Themes**
Current year findings	Mid-market to enterprise	Identified across CIO agendas

EXECUTIVE SUMMARY

The Investment Efficiency Problem in Cyber Security

Organisations across every sector are spending more on cybersecurity than at any point in history. The global cybersecurity market exceeded USD 200 billion in 2024, and Canadian enterprise security spending continues to grow at double-digit annual rates. Yet breach frequency, breach severity, and recovery costs are also at record levels. The conclusion is not that security investment is wasted. It is that security investment is systematically misallocated, concentrated in areas that produce compliance certification rather than genuine risk reduction, and starved in areas where the return on investment in risk terms is disproportionately high.

This research report identifies the five cybersecurity investment areas that deliver the greatest risk reduction per dollar invested for mid-market and public sector organisations operating in the Canadian context. The analysis draws on peer-reviewed research in information security economics, published breach data from major security vendors, Canadian regulatory guidance, and advisory experience with organisations across healthcare, professional services, and public administration. The five investments identified are not the five most expensive security capabilities. They are the five most efficient, producing outsized risk reduction relative to their implementation cost when deployed with appropriate organisational context.

The question every technology leader and board should be asking is not 'How much are we spending on security?' It is 'Where is our security spending producing the most risk reduction, and where are we spending in areas that look rigorous but deliver marginal protection?' These are different questions with very different answers.

The Analytical Framework: Risk Reduction Efficiency

The concept of disproportionate risk reduction is grounded in the economics of information security investment. Gordon and Loeb (2002) established the foundational framework for optimal cybersecurity investment in a landmark paper published in ACM Transactions on Information and System Security, demonstrating that the relationship between security investment and risk reduction is non-linear. Small investments in the right areas can produce very large reductions in expected loss. Large investments in the wrong areas can produce negligible improvement in actual risk posture.

The Gordon-Loeb model and subsequent refinements (Gordon et al., 2015) identify two primary variables that determine investment efficiency: the probability of a successful attack against a given vulnerability, and the potential loss magnitude associated with that vulnerability. Investments that address high-probability, high-consequence vulnerabilities with cost-effective controls produce disproportionate risk reduction. Investments that address low-probability, low-consequence vulnerabilities, or that apply expensive controls to threats that could be mitigated with simpler mechanisms, produce low efficiency.

The five investments identified in this report consistently score at the highest end of the risk reduction efficiency spectrum when evaluated against the threat landscape facing Canadian mid-market and public sector organisations in 2026. They are ordered by the breadth of risk reduction they deliver, not by their cost or complexity. Each can be implemented by an organisation without a large internal security team, and each produces measurable risk reduction within a 12-month implementation horizon.

01 Identity and Access Management

The control that stops more breaches than any other and is most frequently under-invested.

Why Identity Is the Primary Attack Surface

The shift to cloud-based services, remote work, and distributed application environments has fundamentally changed the primary attack surface that adversaries exploit. The network perimeter, once the dominant security focus, is no longer the primary entry point for breaches. Identity is. The 2024 Verizon Data Breach Investigations Report found that 74 percent of breaches involved the human element, including stolen credentials, privilege abuse, and social engineering attacks that exploit identity infrastructure.

Identity and Access Management (IAM) is the discipline of ensuring that the right people have the right access to the right systems at the right times, and that all other access is denied. When implemented effectively, a well-designed IAM architecture stops credential-based attacks, limits the blast radius of compromised accounts through least privilege enforcement, and provides the audit trail that makes post-incident investigation possible. When implemented poorly, or not at all, the entire application and data estate of the organisation is accessible to any adversary who can acquire a valid credential.

The Highest-Value IAM Investments

Multi-factor authentication (MFA) is the single highest-return security investment available to most mid-market organisations. Researchers at Microsoft's security division (Weinert, 2019) analysed account compromise data across millions of enterprise accounts and found that MFA blocked 99.9 percent of automated credential-based attacks. The implementation cost is low, the operational disruption is manageable with appropriate change management, and the risk reduction is among the highest of any security control.

Privileged access management (PAM) addresses the specific risk associated with administrative credentials, which provide the highest level of access to organisational systems and are disproportionately targeted by sophisticated adversaries. The Ponemon Institute's 2023 State of Privileged Access Management report found that organisations with mature PAM programs experienced 50 percent fewer privilege-related breaches than those without. PAM investment is particularly high value for public sector organisations whose administrative accounts may span legacy systems with extensive data holdings.

- Implement MFA across all external-facing systems and email as the immediate priority.
- Enforce least-privilege access principles and conduct quarterly access rights reviews.
- Deploy PAM for all administrative and privileged accounts with session recording for forensic capability.
- Implement single sign-on to improve both security visibility and user experience.

02 Security Awareness and Behaviour Change

Technical controls fail when people circumvent them. Investment in human behaviour change is persistently underfunded.

The Human Layer as Attack Vector

Social engineering, phishing, and business email compromise attacks succeed because they exploit human cognitive patterns that technical controls cannot fully address. Organisational security is only as strong as the least security-aware employee with access to sensitive systems or data. The IBM Cost of a Data Breach Report (2024) identified phishing as the most common initial attack vector in breaches affecting mid-market organisations, responsible for 16 percent of incidents and associated with an average breach cost of USD 4.88 million.

Security awareness programs have historically been evaluated on participation rates and quiz completion scores rather than on behavioural outcomes. This measurement approach has produced a generation of security training programs that are compliance activities rather than risk reduction mechanisms. The emerging evidence base on security behaviour change draws on behavioural psychology and adult learning theory to identify program designs that actually change the decisions people make under realistic attack conditions.

What Effective Security Behaviour Change Looks Like

Workman et al. (2008) published foundational research on the role of social influence and habit formation in security compliance, demonstrating that security behaviour is shaped more by social norms and environmental design than by knowledge of security risks. Effective security awareness programs in 2026 are built on three principles: simulation-based learning that creates realistic decision scenarios rather than passive content consumption; social norm activation that makes secure behaviours visible and valued within the organisation; and environmental design that makes secure choices the path of least resistance.

Phishing simulation programs, when designed and implemented with behavioural science principles, have been shown to reduce click rates on simulated phishing emails by 60 to 80 percent over a 12-month program (Proofpoint, 2024). The investment in a well-designed simulation and behaviour change program is typically less than the cost of a single phishing-initiated breach and produces sustained behavioural improvement rather than point-in-time awareness.

- Deploy continuous phishing simulation with immediate, empathetic coaching for susceptible employees.
- Design security awareness content around realistic decision scenarios, not policy recitation.
- Create visible social norms around security behaviour through leadership modelling and peer recognition.
- Measure program effectiveness by behavioural outcomes, not participation rates.

03 Endpoint Detection and Response

The visibility and containment capability that separates organisations that catch attacks from those that discover them months later.

Why Traditional Endpoint Protection Is No Longer Sufficient

Traditional endpoint security, based on signature-detection antivirus and host-based firewalls, was designed for a threat environment that no longer exists. Modern adversaries use fileless malware, living-off-the-land techniques that exploit legitimate system tools, and polymorphic code that evades signature detection. The 2024 CrowdStrike Global Threat Report found that 71 percent of attacks detected in 2023 were malware-free, using legitimate credentials and built-in operating system tools to conduct their operations. These attacks are invisible to signature-based detection.

Endpoint Detection and Response (EDR) addresses this gap by recording continuous telemetry from endpoint devices, applying behavioural analytics to identify anomalous patterns consistent with attack activity, and providing the investigation and containment capability necessary to respond effectively when attacks are detected. EDR is not a replacement for prevention controls. It is the capability that catches attacks that prevention controls miss, and that contains breaches before they spread across the environment.

The Dwell Time Reduction Imperative

The critical risk reduction benefit of EDR investment is dwell time reduction. Dwell time is the period between initial compromise and detection, during which an adversary has undetected access to the organisation's environment. The IBM X-Force Threat Intelligence Index (2024) reports a global mean dwell time of 194 days for breaches that were not self-detected by the victim organisation. Every day of undetected dwell time represents additional data exfiltration, lateral movement, and privilege escalation by the adversary.

Organisations with mature EDR deployments and active monitoring capabilities have demonstrated dwell times measured in hours rather than months. Laliberte (2020) documented case studies in which EDR-enabled organisations detected and contained attacks within four hours of initial compromise, limiting breach scope to a single endpoint rather than allowing network-wide propagation. The difference in remediation cost between a contained single-endpoint incident and a network-wide breach is measured in orders of magnitude.

- Deploy EDR across all managed endpoints including servers, workstations, and laptops.
- Ensure active monitoring of EDR telemetry, either through internal SOC capability or managed detection and response service.
- Establish documented response playbooks that define the actions to take when EDR alerts are triggered.
- Configure EDR for automated containment of confirmed malicious activity to limit dwell time.

04 Vulnerability Management and Patch Discipline

The uncool control that closes the door before attackers walk through it.

The Persistent Exploitation of Known Vulnerabilities

One of the most consistent findings in breach data analysis is that the majority of successful attacks exploit vulnerabilities for which patches were available at the time of the attack. The 2024 Verizon Data Breach Investigations Report found that exploitation of known vulnerabilities as an initial access vector increased by 180 percent compared to the prior year, driven significantly by attackers targeting unpatched systems that were publicly disclosed months or years before the breach occurred.

The implication is significant: a substantial proportion of the breaches that organisations experience are not the result of sophisticated zero-day attacks or advanced persistent threats. They are the result of failing to apply publicly available patches to known vulnerabilities in a timely manner. Systematic vulnerability management and patch discipline is among the highest-return security investments available precisely because it closes the attack vectors that the majority of actual adversaries rely upon.

Building a Practical Vulnerability Management Program

Effective vulnerability management requires four capabilities working in coordination: asset discovery, which maintains a current inventory of all systems and software in the environment; vulnerability scanning, which identifies known vulnerabilities across the asset inventory on a regular schedule; risk-based prioritisation, which ranks remediation effort based on vulnerability severity and asset criticality rather than treating all vulnerabilities as equal; and patch management, which ensures that approved patches are applied within defined time windows based on risk priority.

The risk-based prioritisation dimension is where many mid-market vulnerability management programs underperform. Organisations that attempt to remediate all identified vulnerabilities equally create unsustainable workloads that result in either burnout and process breakdown or selective remediation based on operational convenience rather than risk. Research by Bozorgi et al. (2010) on vulnerability exploitation prediction demonstrated that exploitability is not uniformly distributed across the vulnerability population: a small proportion of vulnerabilities account for the majority of exploitation activity. Focusing remediation effort on the exploitable minority produces disproportionately greater risk reduction than attempting comprehensive remediation.

- Maintain a current, comprehensive asset inventory as the foundation of all vulnerability management.
- Conduct authenticated vulnerability scans of the full asset inventory at least monthly.
- Prioritise remediation using CVSS scores combined with threat intelligence on active exploitation.
- Define and enforce patch time-to-remediation standards by risk tier: critical within 24 hours, high within 7 days, medium within 30 days.

05 Incident Response Readiness

The investment that determines the difference between a manageable event and an organisational crisis.

Why Incident Response Investment Is Chronically Underfunded

Incident response readiness is the security investment that organisations most commonly defer until after they have experienced a significant incident. The logic is understandable: incident response capability is not visible to external stakeholders, does not prevent attacks from occurring, and does not feature in compliance certification frameworks in the same way that preventive controls do. The financial logic is less defensible. The IBM Cost of a Data Breach Report (2024) found that organisations with incident response teams and regularly tested incident response plans had average breach costs USD 1.49 million lower than those without, a difference that dwarfs the annual investment required to maintain response readiness.

Incident response readiness is not primarily a technology investment. It is a planning, training, and practice investment. The technology components, including forensic tooling, secure communication channels, and backup and recovery capability, are relatively modest in cost. The primary investment is in developing and maintaining the plans, training the people who will execute them, and practicing the decision-making processes that determine whether an organisation responds to an incident effectively or in chaos.

The Three Components of Response Readiness

Cichonski et al. (2012), in the NIST Computer Security Incident Handling Guide (Special Publication 800-61), established the foundational framework for incident response capability that remains the primary reference for mid-market organisations building response readiness. The framework identifies four phases: preparation, detection and analysis, containment and eradication, and post-incident activity. Investment in preparation, the phase that occurs before any incident, is the most efficient allocation of incident response resources.

Preparation investment encompasses three components. First, documented incident response plans that define the roles, responsibilities, escalation pathways, and decision criteria for significant incident types including ransomware, data exfiltration, and business email compromise. Second, incident response training that ensures the people who will execute the plan under pressure have rehearsed their roles in realistic simulation environments. Third, tabletop exercises that test the decision-making of senior leadership, including board and executive participation, under simulated incident conditions.

The tabletop exercise dimension deserves particular emphasis. Most organisations that have experienced significant cyber incidents report that the most costly failures were not technical failures but decision-making failures: delays in escalating to senior leadership, uncertainty about legal notification obligations, inadequate communication with affected stakeholders, and failure to invoke pre-negotiated recovery services. These failures are entirely preventable through well-designed exercises that surface decision gaps before an actual incident forces them into the open.

- Develop documented incident response plans covering the primary incident scenarios relevant to the organisation's sector and risk profile.
- Conduct annual tabletop exercises that include board and executive leadership participation.
- Establish pre-negotiated relationships with a cyber incident response firm for surge capability in major incidents.

- Review and test backup and recovery capability quarterly to ensure data restoration is viable within acceptable recovery time objectives.
- Establish a cyber insurance policy that is specifically structured around the organisation's likely incident scenarios and recovery requirements.

The Portfolio Perspective: Sequencing These Investments

The five investments identified in this report are not independent. They form a coherent security architecture when deployed in sequence, with each investment building on and reinforcing the others. For organisations that are beginning to build their security investment portfolio, the recommended sequencing prioritises risk reduction speed and foundational capability over comprehensive coverage.

The starting point for most mid-market organisations with limited prior security investment should be identity and access management, specifically MFA deployment. This single control addresses the most common attack vector, can be deployed rapidly, and creates the access visibility foundation on which subsequent controls depend. Security awareness investment should begin concurrently, as it has no technology dependencies and begins producing behavioural change within the first programme cycle.

Endpoint detection and response should follow as the second wave of investment, providing the visibility and containment capability that is prerequisite to effective incident response. Vulnerability management formalisation can proceed in parallel with EDR deployment, as it builds on the asset inventory that EDR requires. Incident response readiness investment, specifically planning and exercise activities, should begin before these technical controls are fully deployed, because the planning process itself surfaces gaps and priorities that improve the deployment of other controls.

Security investment is most effective when it is treated as a portfolio management challenge rather than a product procurement exercise. The question is not which security product to buy next. It is which investment, at this moment, produces the greatest reduction in the organisation's most significant risks, given existing capability and resource constraints

Conclusion

The cybersecurity investment efficiency gap in mid-market and public sector organisations is real, measurable, and addressable. Organisations that reallocate investment toward the five areas identified in this report, identity and access management, security behaviour change, endpoint detection and response, vulnerability management, and incident response readiness, will achieve materially greater risk reduction from their security budgets than organisations that continue to invest in the compliance-oriented controls that dominate current spending patterns.

The five investments share a common characteristic: they address the actual attack vectors that are responsible for the majority of real-world breaches in organisations of comparable size and sector. They are not the most visible security controls, the most technically sophisticated, or the most likely to appear in vendor marketing materials. They are the most effective, and effectiveness, not visibility, is the measure that matters when the event the organisation hoped would never happen finally occurs.

References

Bozorgi, M., Saul, L. K., Savage, S., & Voelker, G. M. (2010). Beyond heuristics: Learning to classify vulnerabilities and predict exploits. In Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 105-114). ACM. https://doi.org/10.1145/1835804.1835821

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide (NIST Special Publication 800-61, Revision 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

CrowdStrike. (2024). 2024 global threat report. CrowdStrike Holdings Inc. https://www.crowdstrike.com/global-threat-report

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438-457. https://doi.org/10.1145/581271.581274

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Externalities and the magnitude of cyber security underinvestment by private sector firms. Journal of Information Security, 6(1), 24-30. https://doi.org/10.4236/jis.2015.61003

IBM Security. (2024). Cost of a data breach report 2024. IBM Corporation. https://www.ibm.com/security/data-breach

IBM Security X-Force. (2024). X-Force threat intelligence index 2024. IBM Corporation. https://www.ibm.com/reports/threat-intelligence

Laliberte, M. (2020). Endpoint detection and response: How EDR tools can help detect and contain cybersecurity incidents. SANS Institute Reading Room. https://www.sans.org/reading-room

Ponemon Institute. (2023). State of privileged access management 2023. Ponemon Institute LLC.

Proofpoint. (2024). State of the phish 2024. Proofpoint Inc. https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

Verizon. (2024). 2024 data breach investigations report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir

Weinert, A. (2019). Your Pa$$word doesn't matter. Microsoft Security Blog. https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24(6), 2799-2816. https://doi.org/10.1016/j.chb.2008.04.006

About NexQuad Systems Inc.

NexQuad Systems Inc. is a Canadian enterprise technology advisory firm specialising in cybersecurity advisory, IT governance, digital transformation, technology strategy, and CIO advisory services. We serve mid-market and public sector organisations navigating the complexity of modern technology risk and opportunity. Innovate. Secure. Deliver.

Innovate. **Secure.** Deliver.

www.nexquadsystems.com