BlackBerry. Intelligent Security. Everywhere.

INSIDER THREAT PREVENTION GUIDE

BUSINESS BRIEF

The term insider threat covers a broad spectrum of potential risks organizations face when they allow trusted individuals to access their facilities and information systems. These include risks of theft, physical violence, sabotage, security breaches, and much more. In this guide, we focus on the challenges security professionals encounter detecting, preventing, and mitigating cybersecurity threats from individuals with authorized access to systems and data.

Addressing these challenges has taken on added urgency in recent years due to the outsized impact insider threats have on an organization's overall security posture. According to Gartner[1], insiders are responsible for 50% to 70% of all security incidents and 75% of all security breaches.

INSIDER THREAT ACTOR PROFILES

Who are these risky insiders? Nearly two thirds (63%) of the respondents to a Cybersecurity Insider Survey[2] cited privileged IT users and administrators as the greatest insider security risk. Only 22% expressed similar concerns about "other" IT staff. This makes intuitive sense, since privileged IT users possess both the administrator-level access and knowledge of policy controls needed to exploit vulnerable systems while evading detection.

Only half of the respondents cited concerns about "regular" employees, contractors, service providers, temporary workers, and privileged business users and executives. Far fewer cited executive managers (16%), customers and clients (15%), and business partners (11%).

Risky insiders typically fall into one of three broad categories:

Compromised users who are often unaware that their systems, credentials, or access privileges have been appropriated by an external threat actor.

Careless or negligent users who cause harm inadvertently. For example, a clerk in the finance department may be tricked by a spearphishing exploit into wire-transferring funds into a fraudulent bank account. According to a Ponemon Institute survey[3], 38% of data breaches are caused by employee carelessness. IBM4 attributes 24% of all data breaches to human error.

Malicious or criminal users intent on damaging the organization through theft, sabotage, or espionage. Ponemon[5] attributes 45% of all data breaches to this group. According to Forrester Research[6], malicious or criminal users are often motivated by financial distress, revenge for perceived wrongs, work conflicts, political or religious ideology, and inducements by cyber-criminal and state-sponsored threat groups.

Insider thefts of intellectual property can be particularly damaging. A CSO Magazine article[7] on the theft of trade secrets by a former employee estimated the costs for developing the stolen technologies at $119.6 million.

Many insider security incidents can be attributed to a fourth category: employees with an overweening sense of entitlement. More than three-quarters (80%) of the business decision makers surveyed by Ponemon[8] feel "they are entitled to or should own their work product." Many employees mistakenly believe it's acceptable to take data belonging to a former employer to their next job. According to InfoSecurity Magazine[9], as many as 72% of departing employees admit they do so.

More than three-quarters (80%) of the business decision makers surveyed by Ponemon feel "they are entitled to or should own their work product."

DETECTION CHALLENGES

Risky insiders look very much like their innocent colleagues. They use networks and data to do their jobs. They're assigned privileges and expected to use them productively. In an enterprise environment, this amounts to millions of transactions every day between users and data. How is a security operations center (SOC) analyst to distinguish routine from risky behavior?

To tease out indicators of compromise, some organizations load raw log data into a security information and event management (SIEM) application, where it can be structured, queried, and analyzed with correlation rules. One rule, for example, might fire an alert if a user copies a quantity of data that exceeds a pre-determined threshold from one folder to another. However, rules cannot anticipate every potentially malicious scenario. For example, the rule would not be able to determine whether the data movement was benign (required for the employee to work on a new project) or malicious (a preparation for exfiltration).

Consequently, correlation and other static rules are often noisy, generating floods of alerts for analysts to triage and investigate. Alert fatigue is a common result. In practice, rules-based systems are only marginally successful at extracting actionable threat intelligence from masses of log data. Solutions based on artificial intelligence (AI) and machine learning (ML) technologies are better suited to detecting subtle patterns of emerging threats.

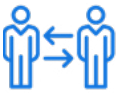
RESOURCE AND MANAGEMENT CHALLENGES

Insider risks have been magnified by the rapid adoption of cloud and mobile technologies and the abrupt shift to a hybrid workforce caused by the COVID-19 pandemic. The number of endpoints has skyrocketed, expanding the attack surface exponentially and exposing enterprise systems to new kinds of threats. Many endpoints used for work are personally owned, poorly secured, vulnerable to abuse, and only partially visible to the SOC.

BitGlass reports[10] that 82% of the organizations it surveyed cannot guarantee they can detect insider threats stemming from personal devices unless they are used on premises (18%) or have agents installed (16%). Half acknowledge insufficient visibility into messaging and file sharing applications on employees' personally owned devices. An equal percentage say they find it harder to detect insider threats overall since migrating to the cloud.

Security teams already over-stretched contending with external threats are often poorly prepared for internal ones. According to the Ponemon[11] survey, issues include:

Resource constraints. Two-thirds (66%) say they lack sufficient funds to manage insider threats. 54% devote less than 20% of their overall budgets to this.



Executive disengagement. Members of the C-suite and board are often unaware of the organization's current insider threat posture. 70% are only briefed annually, upon request, on an ad-hoc basis, or not at all.

Insufficient planning. More than half (54%) lack an insider risk response plan (IRRP). As a result, it takes an average of 118 days for respondents to identify an insider-caused data breach and 55 days to contain it.

BitGlass[12] also cited lack of staff (41%), lack of training and expertise (36%), lack of inter-departmental collaboration (28%), and privacy concerns (10%) as barriers to improvement.

IT leaders surveyed by Ponemon[13] are overwhelmingly downbeat in their post-pandemic expectations for reducing risks of insider threats. 85% say employees are more likely to leak files than they were pre-COVID; 59% expect insider risks to increase in the next two years.

Meanwhile, employees chafe under restrictions intended to bolster security that unnecessarily impair and impede their productivity. Over half (51%) of the IT security leaders surveyed[14] acknowledged they receive daily or weekly complaints from employees who have been mistakenly prevented from accessing their work files.

THE RESULT: RAPIDLY RISING INCIDENCE AND COSTS

The incidence and costs of insider threats have ballooned in recent years. According to Ponemon[15]:

- The number of reported incidents surged 47%, from 3,200 in 2018 to 4,716 in 2020.
- The average per-incident cost increased 31%, from $8.76 million in 2018 to $11.45 million in 2020.

The actual costs vary depending on the identity of the attacker and the nature of the incident. According to Ponemon[16]:

- Although they attract the most notoriety, criminal and malicious insiders accounted for only 23% of reported incidents. However, given the $755,760 average cost, the sum can reach $4.08 million annually.
- Incidents caused by negligent insiders cost organizations the least, "only" $307,111 on average. But since they comprise 62% of reported incidents, the totals can add up quickly to as much as $4.58 million annually.
- Credential theft is a cost multiplier. If the incident involves stolen credentials, the average incident costs nearly triple to $871,686. If the stolen credentials are privileged, the average per-incident cost can reach $2.79 million. Fortunately, only 14% of reported incidents match that profile.

Ponemon[17] attributes the costs to "monitoring and surveillance, investigation, escalation, incident response, containment, ex-post analysis and remediation." Notably, investigation is "the fastest-growing cost center across all incident types, rising 86% in only two years to average $103,798."

The average per-incident costs increased 31%, from $8.76 million in 2018 to $11.45 million in 2020.

BLACKBERRY BEST PRACTICES FOR MANAGING INSIDER RISKS

There's no magic bullet for eliminating insider threats. However, there are concrete steps organizations can take to reduce their frequency and impacts.

- **Baseline the risk environment.** Has an insider incident already occurred? Is one underway? A compromise assessment will answer these questions and provide a detailed roadmap for closing high-priority insider security gaps.
- **Evaluate existing incident response (IR) plans and playbooks.** A playbook for responding to an insider threat may require close coordination between human resources, corporate counsel, law enforcement, and more. Specialized playbooks should be developed and exercised regularly to produce continuous improvements in insider IR performance.
- **Address resource constraints.** Many SOC teams are under-staffed, over-stressed, and suffering from alert fatigue. Organizations contending with resource shortfalls should establish retainer relationships with external IR teams and contract managed detection and response (MDR) services to accelerate incident detection, response, and remediation.
- **Pivot to a prevention-first security posture.** The most efficient way to reduce insider risks is to prevent insider threats from occurring with endpoint protection platforms (EPPs), endpoint detection and response (EDR) systems, and continuous authentication solutions based on AI, ML, and automation.
- **Transition to Zero Trust security.** Minimize insider risks to enterprise resources by treating every user, network, and application as malicious until proven otherwise. Continuous authentication solutions based on AI, ML, and behavioral analytics balance security and productivity, adapting access and security policies dynamically by assessing each employee's up-to-the-minute risk profile.

- **Solve the visibility problem.** The rapid shift to a hybrid workforce has created numerous blind spots in the security fabric. Risks that are unseen cannot be managed. Unified endpoint management and security solutions should be deployed that monitor, manage, and enforce security policies consistently across every kind of device and ownership model.

RISK REDUCTION BEGINS WITH PLANNING AND ASSESSMENTS

First, organizations should acknowledge the strong likelihood that an insider security incident has already occurred or may even be underway. BlackBerry Compromise Assessment (CA) consultants are experts at detecting such evidence, identifying high-priority security gaps, and providing detailed recommendations for remediation. If an insider attack is ongoing, the CA team can transition seamlessly into incident response, helping to trace and terminate the attack and prevent a recurrence. The IR team can also leverage BlackBerry's ISO-accredited forensic laboratory to investigate and analyze forensic data and preserve it in a form that complies with chain-of-custody rules. To address insufficient planning, BlackBerry® Security Services experts can help organizations develop customized IRRPs and playbooks that are explicitly designed to manage insider threat scenarios. If an incident is expected to result in a prosecution, for example, the playbook will specify procedures and guidelines for engaging with legal counsel and law enforcement.

BlackBerry Red Team and Strategic Services consultants can also conduct customized, scenario-specific tabletop and attack simulation exercises that provide invaluable opportunities for SOC teams to build skills and make continuous improvements In their IR performance.

LEADING WITH PROACTIVE PREVENTION

The most efficient way to reduce insider risks is to prevent insider incidents from occurring. This begins with thwarting attempts by external adversaries to gain a foothold on the victim's network, thereby eliminating the downstream costs for tracing, containing, and remediating damage. BlackBerry® Cyber Suite solutions utilize advanced AI, ML, and automation technologies that enable organizations to adopt a prevention-first security posture.

The suite includes BlackBerry® Protect, an EPP that prevents Microsoft® Windows®, macOS®, iOS®, Android™, Chrome OS™, and Linux® systems from being compromised by malware, fileless exploits, malicious scripts, and more. All protection is applied at the endpoint automatically, without any reliance on cloud lookups or a network connection. BlackBerry Protect helps prevent insider threats caused by external bad actors with unparalleled effectiveness, ease of use, and minimal system impact.

ACCELERATING DETECTION AND RESPONSE

A prevention-first strategy must also prove effective at rapidly detecting and mitigating the effects of insider threats originating from malicious and negligent insiders. As noted earlier, this is challenging for static rules-based systems that require every type of policy violation to be defined explicitly in advance. BlackBerry® Optics is a cloud-enabled EDR solution that augments the compromise-prevention capabilities of BlackBerry Protect. BlackBerry Optics utilizes AI, context analysis, and MITRE ATT&CK® framework rules to detect threats from users with legitimate credentials and those who gain unauthorized access by exploiting unpatched servers or insufficiently secured network services, such as Remote Desktop Protocol.

BlackBerry Optics detects subtle signals of an attack hidden within masses of raw endpoint data. Unlike cloud-dependent solutions, however, all detection and response logic is applied at the endpoint to dramatically reduce response latency. The resulting alert, event, and telemetry data is automatically collected, correlated, and stored in the cloud for off-line analysis

When a detection rule is triggered, BlackBerry Optics can respond automatically with playbook-driven workflows that isolate suspect devices, terminate processes, create system images, collect forensic data, assist with recovery and cleanup, and take other appropriate actions to prevent threat actors from achieving their objectives.

BlackBerry Optics enables SOC analysts to initiate containment responses quickly. Reducing dwell time is not only essential for operational resilience, it also benefits the bottom line. According to IBM[18], organizations that resolve incidents in less than 200 days realize an average costs savings of $1.12 million.

REDUCING INSIDER RISKS WITH A ZERO TRUST ARCHITECTURE THAT PROVIDES A ZERO-TOUCH EXPERIENCE

Another key is to adopt a Zero Trust security architecture that controls access to resources dynamically based on continuous assessments of the user's trustworthiness.

BlackBerry® Persona detects potentially malicious activity with behavioral analytic models that learn how users normally interact with their systems and data.

1. **Keyboard models** baseline the time intervals between pressing and releasing a key and between successive keystrokes. The keystroke values are not recorded or retained for analysis.
2. **Mouse models** baseline the time interval between pressing and releasing a mouse button, left and right click patterns, etc.
3. **Log-on models** baseline how users log on to their devices (e.g., locally or remotely) and where they do so (based on anonymized geo-location data).
4. **Process start models** baseline how, when, and where users open software applications.

BlackBerry Persona uses these baselines to continuously compute trust scores that reflect real-time changes in a user's behavior during work sessions. When trust scores are high, access to internal resources can be unimpeded. When trust scores fall below administrator-defined thresholds, access to resources can be reduced or restricted until trust is restored or actions are taken to mitigate the threat.

Like the other members of the BlackBerry Cyber Suite, all BlackBerry Persona detection and mitigation actions are performed automatically at the endpoint, without any reliance on network connectivity or access to the cloud. Typical use cases include:

- **Preventing external threat actors from using stolen credentials.** By comparing the normal behavior of an authorized user to the anomalous behavior of an adversary, BlackBerry Persona can detect attempts to use stolen credentials and take mitigation actions based on administrator-defined security policies.
- **Preventing malicious or negligent insiders from violating access policies.** BlackBerry Persona can detect early signals of exfiltration. Persona analyzes their conduct at the endpoint and determines if their actions are malicious. Malicious conduct will trigger a low trust score, and the attack will be stopped.

BlackBerry Protect and BlackBerry Optics are also available through BlackBerry® Guard, a subscription-based MDR service that provides 24x7 support from BlackBerry incident response and prevention experts.

> ***According to IBM, organizations that resolve incidents in less than 200 days realize an average costs savings of $1.12 million.***

MANAGING INSIDER RISKS FROM REMOTE WORKERS

When workers are remote, it's harder to detect early signals that they're acting unwisely or intentionally violating security policies. That's especially true when the devices they're using are personally owned. Almost all (96%) of the enterprise IT decision makers surveyed by 451 Research19 agreed it was important "to have consistent management and security across all endpoints."

BlackBerry helps reduce insider risks from remote workers by enabling organizations to:

- Centrally manage and enforce policy controls over every device in their fleet.
- Prevent threats from compromising mobile devices. BlackBerry Protect and BlackBerry Persona run efficiently on iOS, Android, and Chrome OS platforms.
- Maintain complete control over digital content while allowing users to share and edit files effortlessly on any device. BlackBerry® Workspaces is a secure enterprise file sharing solution that embeds digital rights management protection into every work file. Content remains secure regardless of where the files are, where they need to go, and who needs to access them.
- Protect the security and integrity of business data with BYOD management solutions that boost productivity and morale by allowing employees to use their preferred devices for work.

KEY TAKEAWAYS

In a perfect world, trust would never be violated. Cyber defenses would be impregnable. No employee would ever behave maliciously or allow their systems to be compromised out of negligence or carelessness. Thus, there would be no need for organizations to monitor or manage insider risks. Unfortunately, the evidence paints a different picture. Insider threats are increasing rapidly in both their frequency and impacts. There are no simple solutions.

BlackBerry recommends that organizations begin by re-examining their existing security controls and processes to assess their suitability for managing insider risks. Next-gen EPP and EDR solutions should be deployed that utilize AI, ML, and automation to mitigate insider threats before they escalate into major security incidents.

Organizations should also transition to a prevention-first, Zero Trust security posture that adapts policies dynamically based on an employee's up-to-the-minute threat profile. And unified endpoint management systems should be deployed that provide SOC analysts with visibility and policy control over every kind of endpoint an insider can use to access enterprise resources.

BlackBerry stands ready to help, with the portfolio of service and software solutions organizations need to reduce insider risks, enhance remote worker productivity, and secure maximum value from their investments in mobile and cloud technologies.

To learn more, visit BlackBerry.com.

1. CISO Magazine: What Edward Snowden Taught Us About Insider Threats
2. Cybersecurity Insiders 2020 Insider Threat Report
3. Ponemon Institute Data Exposure Report
4. IBM Cost of a Data Breach Report
5. Ponemon Institute Data Exposure Report
6. Forrester Research: Best Practices: Mitigating Insider Threat
7. Coca-Cola trade secret theft underscores importance of insider threat early detection
8. Ponemon Institute Data Exposure Report
9. InfoSecurity Magazine: Your Employees are Taking Your Data
10. Bitglass 2020 Insider Threat Report
11. Ponemon Institute Data Exposure Report
12. Bitglass 2020 Insider Threat Report
13. Ponemon Institute 2020 Cost of Insider Threats Global Report
14. Ponemon Institute Data Exposure Report
15. Ponemon Institute 2020 Cost of Insider Threats Global Report
16. Ponemon Institute 2020 Cost of Insider Threats Global Report
17. Ponemon Institute 2020 Cost of Insider Threats Global Report
18. IBM Security Cost of a Data Breach Report 2020
19. 451 Research Pathfinder Report: Securing The Enterprise Of Things

BlackBerry. Intelligent Security. Everywhere.

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 175M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety, and data privacy solutions and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

*For more information, visit **BlackBerry.com** and follow **@BlackBerry**.*