To: John Smith, IT Director

From: Perry Kingston, Security Analyst

Date: June 15, 2025

Subject: **Incident Analysis Brief - Payroll Office Breach & Impacts on Data Integrity**

Incident Summary: On June 12th, 2025 an unidentified and unauthorized person gained access to the Payroll Administrator's office, including her computer system. Physical paperwork was taken during this incident, there are clues that the unknown actor may have utilized a USB device on the Payroll computer and following this event there have been connections to the corporate network from foreign sources, inaccuracies in payroll reports that were generated the day after this incident and there have also been unexplained outages to the payroll application. This brief will assess the impact on data Integrity and propose security updates to mitigate these effects and reduce the likelihood of an incident such as this occurring again in the future.

Security Objective Focus: This incident has a negative impact on all 3 pillars of the CIA Triad (Confidentiality, Integrity and Availability), though the Integrity pillar is most impacted. Prior to outlining the loss of Integrity in particular, it is important to understand how the other pillars are impacted as well. The unknown contents of manila folders which were taken during this event directly impact the Availability of data, as this information is no longer accessible by those who are authorized and need to access it. This incident in itself was a breach of Confidentiality, as a person who was not authenticated and not authorized to access this data was able to successfully interact with it. The Integrity of data was heavily impacted in several different ways; there was potentially tampering of the physical documents in the office beyond the exfiltrated folders, the Payroll Admin stated that the subject appeared to have a USB device and noted that her USB devices had been unplugged so it appears their workstation was disturbed and potentially data was directly modified in the system, along with the possibility of exfiltration. Given the unusual remote connections being made to the system following this incident, the attackers maintain the ability to alter digital records and appear to have done that, evident by the inaccuracies in payroll reports following this event. Integrity is also being impacted outside of this specific payroll data, with unexplained outages taking place which may be a result of malicious modifications of configuration files, database settings and/or application code which indicate a corruption or tampering of critical data resulting in system failures. The loss of data Integrity has the greatest negative impact overall in this scenario as the manipulation of this data doesn't just have a financial cost, but also a loss of trust, regulatory compliance adherence and detriment to continuous business operations. The negative impacts of this event are wide-reaching and impact several different aspects; from a people standpoint this event can cause employees not to be paid appropriately or in a timely manner and causes undue stress to the Payroll Team. From a processes standpoint there have been delays and disruptions in accessing necessary systems and a diminished credibility of internal reporting which coincides with a loss of trust internally. From a technology standpoint, the payroll system is currently unreliable and requires substantial resources diverted in order to resolve this issue, including taking steps to effectively stop further abuse, conduct forensic analysis and also return to typical business operations.

Fundamental Security Principles for Implementation: Two of the most important principles that should be applied to mitigate this risk in the future are instituting Fail-Safe Defaults and Complete Mediation. The principle of Fail-Safe Default dictates that systems should deny access by default and only allow explicitly granted actions. (Saltzer & Schroeder, 1975). In this case, application would take the form of increasing physical security and awareness; office file cabinets should be locked at all times and access to all offices should be denied unless the user provides either a physical key or access badge. Application would also include computer security in the form of devices having screen time lockouts after short idle periods, which would mean any access would require authentication of the user and incorporate Multi-Factor Authentication. This principle can also be applied on a network-level through denying, by default, any connection attempts that originate from unusual or foreign sources. Application of this principle will have an impact on user experience, in terms of people and processes, as there can be slight delays in accessing systems required for operations but this is balanced by a significantly stronger level of protection system-wide. Regarding impacts on technology, this principle does require some overhead to implement but that effort is an up-front cost that is minor in comparison to the negative impacts of a breach such as this. There is also the technological impact of needing to add an Identity and Access Management (IAM) and/or Network Access Control (NAC) system of some sort, to support repeated authentication and authorization in a Zero Trust model. (NIST, 2020).

The second fundamental principle that can mitigate a breach such as this is Complete Mediation, which is the concept that every access request, whether to documents, applications or system resources, must be verified each time it occurs and not only at the initial point of authentication. This ensures no assumption of ongoing trust and instead requires every action be explicitly authorized. This concept works hand-in-hand with the Fail-Safe principle by ensuring that access is denied by default and that any access which is permitted will be continuously validated. Together, these two principles will not only prevent unauthorized access passively, by default, but also actively, through repeated verification, and the combination significantly reduces the risk of ongoing exploitation even in the event of a compromise such as this intruder gaining access to the Payroll office and systems. In the case of this incident, having Fail-Safe policies in place could have prevented the attacker from accessing these files and systems in the first place and even if they managed to compromise the office and gain unauthorized access, having Complete Mediation implemented would have made it significantly more difficult for the attacker(s) to continue accessing the system remotely and continue to cause disruptions to normal business operations, by requiring authentication at every attempted access of assets.

Ideally both of these principles should be immediately implemented but if there is the need to prioritize only one of these two fundamental security principles, it should be Fail-Safe Defaults. In this event, with a suspicious individual entering an unauthorized area and then exiting through an emergency door, there was no mention of the use of access badges, physical locks and keys or alarms being triggered and a Fail-Safe Default system would have required that these physical doors were locked and required a token held by an authorized user to enter. Upon entering the office, the attacker was able to abscond with physical files and also gain access to the computer system, both of which actions would have been made more challenging through Fail-Safe Defaults by having all physical files locked within secure filing cabinets, and the Payroll computer being locked which requires a successful login to manipulate the system. This principle is part of Layering/Defense-in-Depth and in this case could have prevented this person from accessing sensitive information, on both physical and digital layers.

Below is a summary of key findings and recommendations.

Synopsis & Key Takeaways:

- Primary Security Objective Impacted: Integrity; due to manipulation of payroll data and corruption, potential document exfiltration and ongoing system disruptions.
- Impacts on Teams: Payroll Team stress, potential impacts on employee pay, decreased employee trust.
- Impacts on Processes: Disruption of crucial internal reporting, reduced access to necessary systems, constrained workflows.
- Impacts on Technology: Ongoing system disruptions, potential presence of malware and requirement of resource allocation for remediation and recovery.
- Recommended Principles to Reduce Future Recurrence:
    - Fail-Safe Defaults: Deny access by default; locked doors, secure logins etc.
    - Complete Mediation: Verify every access attempt continuously, not just at login.
- Priority Recommended Update: Implementation of Fail-Safe Defaults to immediately reduce the risk from unauthorized access and strengthen perimeters of system, both digitally and physically
- Next Steps: Institute IAM/NAC systems for consistent user authentication, improvement of physical access controls, implementing stricter controls in the network regarding unusual login attempts, mandatory security-awareness training for all employees.

These measures will strengthen the organization’s ability to maintain operational integrity, business continuity and enable effective mitigation of future security incidents such as this.

References

Saltzer, J. & Schroeder, M. (1975). *The Protection of Information in Computer Systems.* University of Virginia, Department of Computer Science. https://www.cs.virginia.edu/~evans/cs551/saltzer/

Rose, S., Borchert, O., Mitchell, S. & Connelly, S. (2020). *Zero Trust Architecture (SP 800-207).* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf