Packsize Final Project Report

By: Valeria Brochero, Madison Barker, and Alexander Rodriguez

Executive Summary

The forthcoming document describes Packsize's IT infrastructure in detail and highlights key points in the business' operations. It is meant to dissect the policies and procedures currently in place, and ultimately provide insight to possible solutions that could positively impact both maintenance and response efforts. The idea is to standardize processes as the organization grows exponentially, and ensure these solutions are scalable to grow alongside the business. The current architecture is rather lax, inadvertently providing a larger margin of human error by leaving decisions up to personal discretion. We understand that this implies risk but that there are inexpensive changes that can be made which will mitigate and perhaps eradicate said hazards.

These changes include: the implementation of a scheduled newsletter to inform all employees of important security measures to adopt or the creation of a new company-wide policy. Stronger creation and enforcement of said policies to reference for repeat issues. A specific, SETA compliant channel to report incidents in a timely and formal manner, to aid in efficient response. Along with a mixed asset naming convention to better distinguish and categorize company-issued equipment. These areas of improvement will undoubtedly bolster Packsize's response efforts, and simultaneously limit risk.

Table of Contents

Introduction

Business Overview

For our company project we decided to analyze the IT infrastructure at Packsize. Packsize is a company that specializes in right-sized packaging solutions for its customers, from small mom-and-pop shops to corporate giants such as Walmart and Home Depot. Packsize follows a business-to-business model as it holds distinct service level agreements with each of its customers, where a custom solution is built for them and their specific needs. This workflow is then integrated into the customers' existing warehouse management system, providing a seamless merger between the two systems, which allows production to be run and tracked in a database known as 'Packsize Reporting'. This optional software aggregates information such as amount of raw material used, boxes produced per hour, and total downtime, which helps organizations track their progress to reduce their carbon footprint. It also helps these customers identify gaps in their own processes by providing valuable insights, which they may then fill to improve efficiency; something only possible through the use of this added visibility. Evidently, Packsize was built on the fundamentals of sustainability and waste reduction in a world that is increasingly dependent on e-commerce and packaging. It was founded by Hanko and Laura Kiessner back in 2002 and currently has around 700 employees worldwide. Its main offices are located here in Louisville and in Salt Lake City, Utah, with machine manufacturing taking place in Sweden.

Our point-of-contact for the IT department in Louisville was Madalyn McCormick. She was recently promoted to Helpdesk Supervisor and is involved in the deployment of hardware and software while also addressing technical issues that may arise for employees. Highlighted in this report will be topics that she shed light on such as end-point security, protection and detection, incident response, disaster recovery, and asset identification. The disaster recovery plans specifically were a topic of discussion which promoted us to meet Chris Langer, a tier 2 systems administrator in the Salt Lake office. He was able to provide deeper insight into the plans, how these systems are tested, and who is involved in this process. After 2 brief zoom meetings with Madalyn and a bit of Chris' assistance, we had all the information needed to elaborate on their IT architecture and make suggestions that suit the organization's needs.

Current Cybersecurity Training

The current cybersecurity training offered to Packsize employees is rather brief. It consists of a 30-minute course housed on a learning platform called *Bridge*. However as of this week, Packsize is moving these resources to a new platform called *Seismic*, that will not only house all trainings, but also includes articles needed for customer support. The current course must be passed with at least 80% accuracy, which takes roughly 30 minutes to complete. This is paired with an annual mock phishing email which is secure way to conduct training exercises under supervision of IT staff. If an employee fails to recognize the phishing attempt and clicks on the link, additional completion of the 30-minute security course will be required.

Software

During our first meeting, Madalyn informed us that they outsourced software called *Sophos* as an endpoint protection and security system. As of our second meeting, they switched to a software called *SentinelOne* to act as their endpoint security system. They also hired a third-party security and consulting organization called *eSentire,* who has access to all their systems and provides 24/7 monitoring as part of the agreement. *ESentire* also delivers regular audits and can help determine the validity of an alert. They do this through the use of descriptive logs which provide an insight deeper than what Packsize is capable of alone. This allows the organization to transfer responsibility for fine-tuning systems and monitoring alerts, which resolves the issue they were experiencing with an overwhelming number of false positives. After receiving the threat alert, the critical infrastructure team would be engaged to help isolate any affected machines from the network, containing and eradicating the threat.

Another set of software required on endpoints to secure remote connections is a VPN (Virtual Private Network). Using a VPN when working remotely is important because it encrypts traffic to the company network, which is common practice for the organization. They also use a *Nutanix Cloud Cluster* for their developer teams and testing software. This software is used to provide scaling, intelligent cloud infrastructure, auto host remediation, and intelligent workload placement.

Hardware

When an employee starts at Packsize, they are given a company issued laptop. This laptop is then asset tagged with the device's serial number. Upon first setup the owner is assigned, and encryption of the hard drive is completed along with the installation of anti-virus which is standard for all endpoints. They accomplish this using *Windows Autopilot* which automatically configures the machines once the user signs into the device, streamlining the initial issuing of hardware. Departmental profiles are used to ensure that all employees will have the necessary software to perform their required duties, while also controlling software inventory for those that have task-based needs. Amongst this configuration we can find *Okta,* an identity and access management provider also used by the organization. It helps deploy new software quickly and displays it for the teams who need it, and was most recently used to introduce Seismic. It also serves a two-step process verification through the use of its application, *Okta Verify*.

Current Risk Mitigation Strategies

One of the ways that Packsize mitigates their risk is by requiring all software downloads to be approved by a member of their IT department. Software installations require a formal request for review and approval, which is then completed by an IT administrator who remotely connects to install using their own credentials. By having all installations completed by IT administrators, we greatly reduce the risk of malware being downloaded and it prevents the use of pirated software too.

Another risk mitigation strategy is the implementation of physical access controls to their building. This keeps their facilities secure by reducing the risk of unauthorized access to data, hardware, or documentation and the risk of a physical attack. They do not have a distinct facilities management team, thus these tasks are left in the hands of the IT department. They have an established way of doing this by creating physical badges for employees. However, they have noticed that the creation and printing of these physical badges is costly and time-consuming, especially for employees that are not local to the area and do not require extended access. To be more efficient in their physical access controls, they are switching to a mobile application provided by *Verkada*. This application will allow current employees to access the building by entering their company credentials directly into the app. This will allow Packsize to quickly grant and remove access to the building for temporary visitors.

Newsletter: Suggestions

Since Packsize does not have a strong SETA program in place, we suggest supplementing this information into a weekly or monthly newsletter that can be sent out to all employees. Newsletters are an effective way to raise awareness on cybersecurity and ensure that it stays on the mind of employees. Employees often create cybersecurity issues unknowingly within an organization, such as falling victim to phishing, not following organizational policies, or making mistakes due to lack of training. A newsletter can address the risk of employees not being knowledgeable of threats or organizational policies. One thing that we were told is that their IT department does not have an excess amount of time or resources available, so a newsletter would be a quick and cost-effective way to promote a culture of security within the organization. Packsize does have a learning and development team that is responsible for the creation of their cybersecurity course, and collaboration between the two departments and even a bit of reviewed AI would help easily implement this into the organization.

The contents of these newsletters can include links to articles related to cybersecurity, to transfer some of the required work to other sources. It also would be a smart idea to include tips on how to practice good cybersecurity habits, recognize common threats, directions on how to report incidents, and policy and procedure updates as the documentation is reviewed. Including these contents in a newsletter enables the organization to promote real actionable steps for employees to take which improves awareness and fosters a culture of security.

Policies and Enforcement: Suggestions

Another issue that we found when speaking to our representative at Packsize, was that they do not have a published list of standards and policies. The creation of our recommended policies is crucial because this lays the foundation for current and future planning, design, and deployment. A repository of standards and policies will give employees a way to reference official documentation when questions arise and enable management to enforce directives uniformly. Packsize's technical teams have developed de facto guidelines which they operate under, but the organization seems to lack policies originating from the enterprise level. Madalyn told us that they have monthly meetings and updates on security incidents, and that security has a good relationship with other key leaders. Since policies should originate from the top, we believe during these meetings, they could begin drafting organizational policies and review current procedures.

For the content of these standards and policies we used the University of Louisville's policies and standards list. At a minimum their written policies should include user accounts acceptable use, data encryption, workstation and computing device standards, password standards, security incidents, business continuity and disaster recovery, and email usage. These policies must be agreed upon by executive leadership and reviewed and updated at set intervals. This is important as it ensures that the information listed in the policies is current and relevant to the organization and its systems.

One of their main drawbacks in the creation of written policies is that they feel that they would have trouble enforcing them. While having a written policy is good, the policies are not effective unless they are realistic with the organization's culture. Madalyn didn't seem to think there was any way to enforce policies if they were published, but policies are the first step in the right direction, but it is ultimately up to management when it comes to uniformly enforcing policy. The reading and review of these policies should be a part of their onboarding process for new employees, and they should be formally agreed upon at the start of employment.

Testing Phase: Suggestions

Another problem that was brought to our attention by Madalyn is that she felt like since things in the organization were evolving so quickly, they have not had enough time for a testing phase. They currently use the *Nutanix Cloud Cluster* for developers to perform testing, but there is not a current testing phase or system for employees who are working with the system. Within the short amount of time in between our meetings, they had made several changes to their cybersecurity plans and the software that is being used. Not giving employees enough time in the testing phase can lead to bugs in the system, resistance to change, and ineffective implementation of new software and systems. It is important to test systems before implementation and to validate that all systems are working as intended.

One way for Packsize to give employees more time to test a system is to utilize parallel or phased conversion strategies when possible. Based on what we learned, they use direct changeover in most cases, because in just last few months there have been making changes with little to no testing in a changeover period. A parallel conversion strategy is when two systems run concurrently with each other, but it is often times the most expensive testing method. However, this would give employees time to adjust and test a new system while still having the old one in place to failback on in case of any failures or if changes need to be made. Once the new system is successfully implemented and tested for a reasonable period of time, the organization could then stop using the old system all together.

Reporting Channel: Suggestions

During our meetings with Madalyn, it became clear that Packsize was taking steps to address the response area of NIST's cybersecurity framework, but we realized that one small addition would be helpful for all parties involved. When the question "how do internal team members report incidents?" was asked, Madalyn indicated that informal channels like chat or email would be used to contact someone from IT. Creating an easy way for team members to establish a formal channel with the appropriate CSIRT teams would reduce response time during the identification of an incident and improve accuracy of documentation. It would accomplish this by avoiding potential confusion when contacting CSIRT teams and validating information during initial detection. A response form would take out the guess work of contacting CSIRT teams, because it would allow the incident response team members to provide their official contact information and automate it appropriately. This means the form would be tied to a distribution list in their email system containing the designated personnel and could even tie into a ticketing system, which would act as the primary trigger. Next, accurate documentation of the reported incident would allow said response teams to effectively triage the incident with a quick glance, reducing the amount of initial investigation required to determine the scope. Instead of receiving a message or email with paragraphs of potentially unnecessary information, the proposed forms would provide fields suitable for incidents only.

The importance of structured responses and the ability to automate communication and capability of form responses is rooted in the professional experience of the group. The goal of incident response is for security teams to respond quickly to minimize disruption of services and document findings for further analysis. This suggestion would be an actionable step to implement even provided limited resources, and it would empower internal users to self-identify events that could be considered incidents. This is key because not all incidents come in the form of alerts on an IDPS system, and could be more so a violation or imminent threat of violation of security policies.

Questions on the form would help identify the scope of the incident, the type of incident, the trigger of the event, list all individuals involved, and confirm accurate contact information. While it may be rare for non-technical staff to report incidents, it would be a low-cost solution which enables reports to be sent directly to key technical staff. Once the form is created, it can be shared throughout the organization which will equip employees when security concerns arise. One downfall could be the potential misuse of the form due to the ignorance of non-technical staff, which could lead to unnecessary notifications. The best way to avoid this is by providing context to the form and carefully structuring the form. When someone is filling out the form and they don’t see a drop-down selection for the issue they’re reporting, then it should occur to them that they may not need to report the issue as an incident. If a description of the form’s intended use is provided along with the link, or even on the form itself, then misuse of the form should be comfortably avoided.

Disaster Recovery: Suggestions

During the meetings with Madalyn, it became apparent that IR and DR plans were not discussed with helpdesk teams. When asked about them, the answer was “I am sure they exist” (McCormick, 2024) which was later confirmed by Chris Langer who works in their infrastructure team. Chris went on to say that DR exercises involve mostly a small group of infrastructure admins who find ways to “break” or shut off systems, to simulate a real event (Langer, 2024). This allows the appropriate teams to respond and conduct the plan that best corresponds to the impact. The response from Madalyn indicates that these plans, practice, and reviews do not include the helpdesk which is somewhat alarming in some ways. This is good in a way because it means that segregation of duties is being maintained, and only identified key roles are participating. However, the helpdesk will be involved in recovery efforts despite proper backups which occur daily. Although the helpdesk will not be active in network recovery or other infrastructure systems, in major incidents or disasters they would likely be involved in the IR, DR, or CP plans. This is because the helpdesk interfaces with personnel who are responsible for the nontechnology functions and would be responsible for the computer recovery aspect of because this involves the physical computing assets which they manage.

Firstly, pieces of the contingency plans should be published internally for personnel to review in case of a major incident or disaster. The fundamental reason that these plans exist is to ensure that guidance is in place for critical systems to be recovered to continue operations. While key leaders and select system admins will be responsible for major technical efforts, it is still important to be transparent so that individual members can support and reinforce the importance of the plans. If Packsize were to increase the level of involvement that the helpdesk has during plan review and practice, it would also increase the thoroughness of these plans. This will ultimately benefit the organization because it will more effectively identify gaps in planning and improve overall effectiveness.

One could argue that during the business impact analysis, it was determined that the mission/business processes were not critically dependent on computing assets that the helpdesk are primarily responsible for. While this topic was not discussed during our research, there is an expressed level of confidence that the business has evaluated the impact on profitability, impact on revenue, impact on market share, etc. for each of their systems. Though, even if the computing devices are rated as a low asset priority, they are still assets nonetheless and there are still scenarios where the helpdesk would be needed in select contingency plans. At the very least, Packsize’s infrastructure teams could discuss recovery resource requirements with helpdesk leaders, to ensure that the appropriate resources are available if computing assets needed recovery. This would include reviewing and documenting the projected costs along with the descriptions of their assets.

Hardware Inventory: Suggestions

Currently Packsize manages their hardware inventory utilizing a naming convention that includes the serial number of the computing machine. Though this is a good unique identifier for these assets, there are some improvements that can be made which will allow technical teams to identify them more quickly, and efficiently manage a central repository. The suggestion is to use a mixed naming convention that utilizes asset tags or serial numbers, along with abbreviations for the system or model type and domain or location that the asset resides in. This not only works for computing machines like endpoints, but also for servers and other systems storing, transmitting, or processing data. The location/domain is important when dealing with multiple locations like Packsize, who operates globally, because administrators are commonly broken into groups that manage their own segment. Each administrator group has their own set of responsibilities and capabilities, so quickly identifying the systems owner will allow for timely responses. The inclusion of system or model types is useful because this helps technical personnel recognize what type of system they're dealing, allowing them to proceed accordingly. The handling of alerts or other tasks, for example on a laptop versus a server, will be different which is why it would be a good idea to have an identifier in the naming convention. This all aims to improve the capabilities of internal teams to identify the asset's official use and administrator or owner by using logical and physical differentiators.

One other less critical reason to remove serial numbers from the naming convention altogether and use something like an asset tag would be to minimize human error. One could argue that in large quantities, the use of serial numbers could increase the likelihood of human error as opposed to something like an asset tag which often comes with a barcode. Another note is that serial numbers are structured differently depending on the manufacturer and model, which could affect efficiency while managing large sets of assets during configuration control and patch management.

Conclusion

To conclude, many factors must be considered when building an ideal infrastructure to host our systems and store data. What is the cost of our sensitive information to the organization, and how does it compare to the price of a robust solution. A cost-benefit analysis must be performed to determine the right amount of security measures to implement. Additionally, it's important to note how the solutions we choose can be scaled as the company experiences growth. At Packsize policies and procedures tend to change very quickly, and it seems that not everyone is equally informed about said changes. Taking all of this into consideration, we have opted for 4 simple yet effective solutions to maximize communication and efficiency amongst all teams.

The first is the implementation of a cybersecurity newsletter as a method of consistent communication to all departments. This responsibility could be rotated amongst the members of the IT dept to include useful links to relevant articles and/or new policies as they are created. It does not have to be long and can even be partially AI generated to reduce the hassle. We understand that time is a concern at any organization, but we believe that this small sacrifice would help Packsize and its employees long-term.

As mentioned, we would also like to observe more structured policies and active enforcement starting from the top. As a company experiencing exponential growth, Packsize cannot afford to continue to respond to different scenarios as-seen-fit. These will later turn into discrepancies and both internal and external stakeholders will have different expectations of what constitutes an adequate response. As we've recently seen, the move to *Seismic* demonstrates that the company understands where its limitations are, and that the more we can standardize our processes the better. This reduces risk and human error.

The use of an incident reporting channel would also be beneficial in the disclosing and triaging of potential and active threats to the system. It would automatically request necessary information as part of the form, and it would allow for a more formal response.

This system could also trigger a timer to start once a report is submitted, and display who has been assigned to assist, for transparency purposes.

Lastly, a mixed asset naming convention has been proposed to aid in locating and maintaining view of all company-issued assets. We suggest that the new method use both model numbers as well as geographic indicators to help with efficient tracing. In addition to this benefit, it will standardize the names to be more congruent, and aid in patch deployment. We are confident that by implementing the above changes, Packsize will achieve a denser, yet cleaner IT infrastructure that will directly benefit its employees, and by default its' customers as well.

References

Langer, C. (2024, 04 16). Infrastructure Engineer. (V. Brochero, Interviewer)

McCormick, M. (2024, 3 22). Helpdesk Supervisor. (V. B. Alex Rodriguez, Interviewer)