Change Management In Cybersecurity

Introduction

Given the dynamics that are happening today, primarily driven by the Remote Workforce and the resurgence of COVID19, IT Security teams have to be able to respond to change quickly in order to keep up. But not only this, they must also have a history of what was happened in the past so they will know what has worked and what didn't in order to make the best decisions possible going forward.

This is the role of Change Management and is the focal of this article.

What Is Change Management?

In a technical sense, Change Management can be defines as the requesting, the approval, and the logging of all sorts of changes to both digital and physical based assets in your IT /Network Infrastructure. In this context, there are three broad categories of changes, which are as follows:

1) The Standard Changes:

   These are changes that happen on a routine basis, with some level of approval required. Examples of these include swapping out hard drives, putting in new memory, or even simply creating more space on a web or database server. These kinds of changes are quick, and barely have an impact on the day to operations of the business. Normally approval from a team lead is all that is needed.

2) The More Complex Changes:

   These are the events that require more to accomplish, and there could be minimal downtime (perhaps no more than an hour or so), and are typically done in the after business hours or on the weekends, in order to minimize the impacts to employees. Some examples of these include the installation and deployment of new controls to safeguard your assets, adding more network security tools to beef up your lines of defenses, and even doing some partial migrations to a cloud based infrastructure. These kinds of events typically have to be tested in a sandbox environment, before they are moved out to production. Higher levels of approval are needed in these instances, such as the manager of the IT Security Department.

3) The Drastic Changes:

   These are the events that happen all of a sudden and at a moment's notice, without any kind of warning. Typically these are the Cyberattacks or other forms similar incidents (even natural disasters) that can cripple an entire business. The downtime can be much longer, ranging from a few hours to even a few days. The goal here is to bring up the mission critical processes as quickly as possible, relying heavily upon both the Incident Response and Disaster Recovery Plans. Any approvals here occur at the highest level, namely that of the C-Suite, especially that of the CISO.

The Key Benefits of Change Management

Some of these are:

1) Changes can happen quicker:

By keeping a detailed log of how similar changes were accomplished in the past, the IT Security team can deploy newer ones in a much more seamless fashion, decreasing the downtime even more. Of course, even as the newer implementations have been installed, the process of how it was all done will need to be documented as well for future use/

2) A historical record is kept:

   The primary benefit of this has already been pointed out, but keeping detailed logs, this come in very useful as well in case your company is ever audited by regulators. By showing such documents, you can prove that you and your IT Security team have taken proactive steps to keep all confidential information and data safe, and are continuing to do so on a regular basis. This will help to lessen the chances of a steep financial penalty, and also, these kinds of documents will have to be produced if you ever apply for Cybersecurity Insurance.

3) You can go back into time:

   Suppose that you have implemented a new control for a digital asset, but for some reason or another, it is not working to its optimal level, even despite all of the prior testing you did to it. In these cases, you will want to roll back this new deployment into a previous state of time in order minimize any further risk that it could bring. By having a log, or history of how this deployment happened, you can roll back to any instance that you need to very smoothly, in a short period of time.

4) Clear communications will be established:

   By maintaining a detailed history of what has happened to particular instance, and what is planned for it in the future, all key stakeholders will be kept informed in an open and transparent fashion. Typically, these documents are reviewed in Change Management meetings, which happen on a preestablished basis. At these venues, everybody involved can share their thoughts as to how a certain process worked in the past, and perhaps what could be done better going forward. That way, there is a common consensus amongst all of the parties that are involved.

5) It can help reduce downtime:

   At the Change Management meetings, all of the impacted parties can voice their concerns as to how their systems will be impacted by it. For example, if a new payroll system is going to be installed, reps from the Accounting, HR, and Finance departments can come to these meetings, and come up with a plan with the IT Department as to the best way this should be deployed, especially the timeframe in which should occur. This dialogue should be recorded into Change Management log files, so there will be a detailed reference for when this deployment should actually occur. By following this methodology, it will help to further reduce the downtime that will be experienced.

Conclusions

Overall, this article has examined what Change Management is, why it is important to your business. This is just as important as requiring your employees to maintain strong levels of Cyber Hygiene. After all, given the virtual world we live in now, the last thing you want is your IT Security team to be guessing

what to do in the case of a security breach. They should have a record of the past to mitigate and correct the events that are happening in the present.

Sources

1) https://www.cioinsight.com/it-strategy/it-change-management/