The Ineffective Control Zone

2018 Edition

A Consequence of Ineffective Controls

Lack of 2nd Person Review

On an early Saturday morning in January, the Hawaii Emergency Management Agency conducted a missile alert drill. The person who was asked to kick off the drill believed that it was an actual alert and selected the wrong option from the menu. This led to 38 minutes of mass panic within the state.

An after-the-fact review found that:

- The system did not have any different visual queues between the test option and the real option (causing confusion).
- The system did not require approval by a second person or a supervisor which means that a single person could initiate an alert causing a panic either accidentally or intentionally.

To address these issues the agency has changed the system workflow so that two analysts must sign in and validate an alert (drill or real) for it to be acted on. The agency is also looking at changing the interface to make it easier to identify test versus production.

A Consequence of Ineffective Controls

Lack of Known Plan For Handling False Alarms

After the incoming missile alert was sent and the team in the command cent realized the mistake, there was confusion on how to send a false alarm alert. To further confuse matters, the drill occurred during a shift change and since the incoming shift leadership had not been notified of the drill, they thought the alert was genuine. These factors led to a 38 minute delay in sending the false alarm alert.

To address these issues the agency:

- Has established a procedure for handling false alarms and set up templates in the system for them so that "all clear" alerts can be sent without delay.
- Will no longer run drills during shift changes and will notify all supervisors of drills in advance.

A Consequence of Ineffective Controls

Writing Down Passwords

In the aftermath of the Hawaii missile false alarm, the agency gave the press a tour of the command center they run. A photograph taken on the tour captured a sticky note stuck to a monitor containing what looked like a password. An agency spokesperson confirmed it was a password to a "minor system that is no longer in use." When passwords are written down and visible:

- Anyone can log in as that user – Loss of accountability.
- Unauthorized persons can now gain access to system.
- Authorized users may now be able to bypass review and approval controls by submitting a request under one ID and then approving it as another.

A Consequence of Ineffective Controls

Robot Programming Testing Failure

Impact:

293 SUVs had to be replaced (scrapped) at a cost of nearly $9.4 Million.

SUBARU

Due to "improper software programming for the welding robots," key structural spot welds were missed on the B pillar between the doors. The missed spot welds may have weakened the overall strength of the SUV body and increased the risk of passenger injury in a crash. Fortunately for Subaru only 9 of the 293 affected SUVs were sold to customers or this could have been MUCH MUCH worse. Please keep in mind that robots do only what we tell them to do. This is what can happen when an error or typo exists in a single line of code and we don't perform sufficient testing within QA to detect it.

A Consequence of Ineffective Controls

Improper Storage/Handling of Employee Records

Breach Impact:

Unknown and we may never know the full extent.

When Toys R Us liquidated and shut down its remaining stores in mid 2018, it looks like at least some locations did not invest the time required to dispose of or secure employee records maintained in the store. These records have been found in some locations just laying around out in the open and contained names, addresses, pictures of driver's licenses and social security numbers. For affected employees, adding to the insult of losing their job, the company also injured them by exposing their data through the company's negligence and /or apathy! SHAMEFUL!

A Consequence of Ineffective Controls

Forgetting to Perform A Critical Manual Control

Impact:

30 passengers fell ill and required treatment.

JET AIRWAYS

In September 2018, a Jet Airways flight took off for Jaipur and had to turn back and make an emergency landing in Mumbai after 30 passengers fell ill due to a lack of cabin pressure. An investigation determined that the flight crew failed and possibly forgot to turn on the system that maintains cabin pressure automatically.

A Consequence of Ineffective Controls

Lack of a Viable Audit Trail

HABERSHAM COUNTY
GEORGIA | Est. 1818

Impact:

Without a paper audit trail on ballots cast, hackers can adjust the results without detection which calls the integrity of the vote into question.

Electronic voting machines are simply computers tracking and tabulating input (votes). As hackers become more sophisticated and more devices including voting machines are connected to the internet, the risk of voting results being altered by hackers increases. To protect against tampering, most electronic voting systems maintain a real-time paper audit trail/log of each vote when cast so that tampering with totals can be detected and invalidated. There are however fully paperless electric voting machines used in 4 states including Georgia. In a recent election, one precinct using these machines had 276 registered voters and 670 votes cast (243% voter turnout) and yet the state of Georgia claimed in its defense of a federal lawsuit for using these voting machines was that there are no issues or gaps. Furthermore, the Georgia legislature attempted to criminalize security research into the voting machines that identify gaps and weaknesses that hackers could exploit. Fortunately, the governor vetoed the effort.

A Consequence of Ineffective Controls

Lack of Software Patching

Impact:

tsmc estimates it will take a $250 Million dollar hit in combined remediation costs and lost/delayed production/sales.

In mid 2017, the ransomware software WannaCry was released. It took advantage of Windows vulnerabilities that Microsoft had issued patches for in early 2017. Despite the numerous highly publicized WannaCry attacks in 2017 and the availability of the patches, tsmc, the world's largest chip maker who supplies apple, AMD and others, chose not to patch their Windows 7 systems. In august 2018, tsmc was infected by WannaCry and has estimated that it will cost the company $250 million.

A Consequence of Ineffective Controls

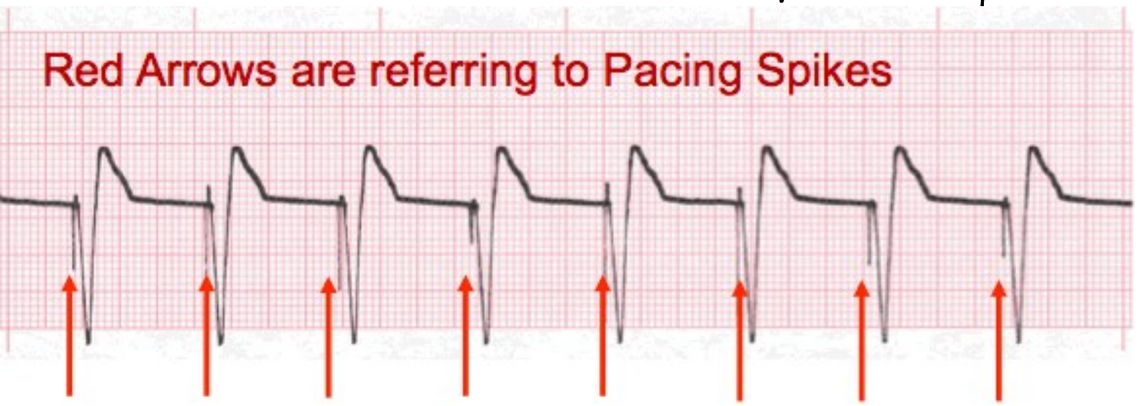
Not Patching Newly Smart Devices

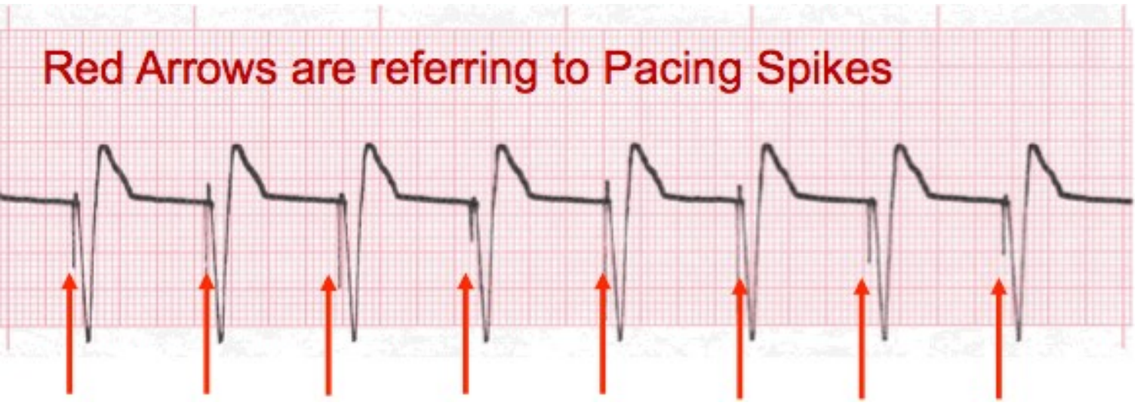
The TV is Watching You

In recent years, formerly single use devices such as phones, teleconferencing units, cameras and televisions (especially those used at high end hotels and conference centers), became more sophisticated, powerful and flexible. This was due to the inclusion of computing components and smart applications being installed. As is the case with any computing device, it can have vulnerabilities that can be exploited and must be patched/maintained. Some of the known exploits in the wild allow a hacker to take over these devices and use the built-in cameras and mics to spy on the room. Unfortunately, because people still see these devices as single use and dumb, they are generally overlooked when it comes to reviewing systems to ensure they are properly secured and patched. This leaves these devices open to exploit! We must change how we think of them and treat them like any other computing device!

A Consequence of Ineffective Controls

Lack Of Focus On Security





Impact:

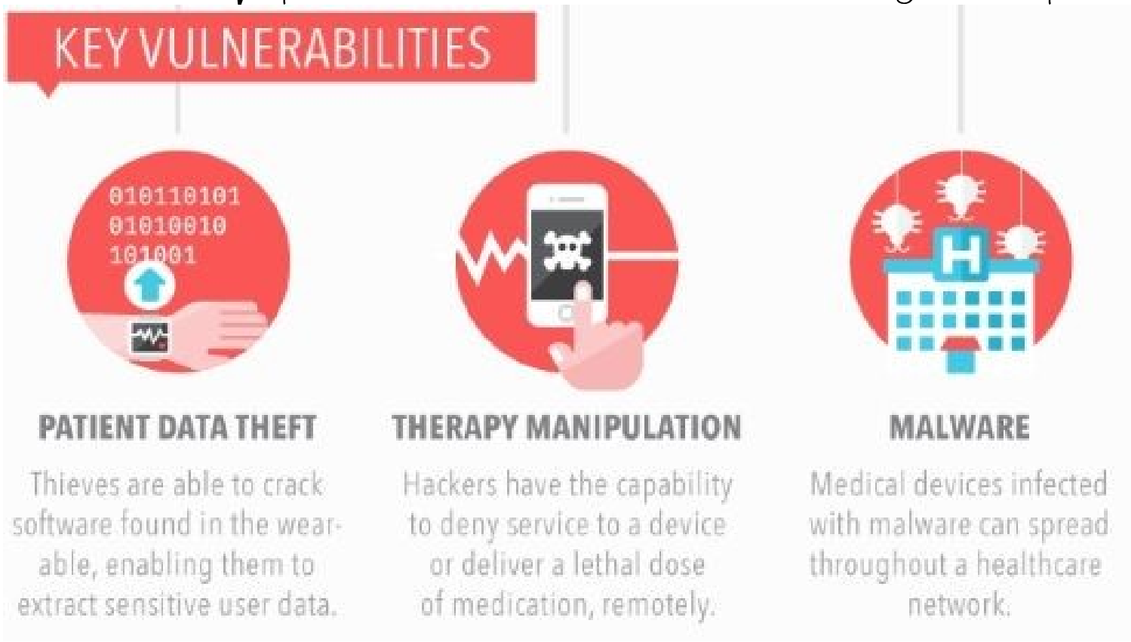
Anyone with an affected pacemaker is vulnerable to attack. Modern pacemakers have the ability to be updated/tuned via an application without subjecting the patient to additional surgeries. However, researchers believe they have discovered that the update process used by Medtronic pacemakers is not secure and can be hacked. The hacker would then be able to change the operating instructions for the pacemaker to change when and how shocks are delivered so that it can deliver unnecessary shocks, withhold needed shocks or change the intensity of delivered shocks. Since the pacemaker is a critical life saving device, this is a matter of life and death!

A Consequence of Ineffective Controls

Lack Of Focus On Security

Impact:

Medical equipment is vulnerable to hacking/manipulation putting patients at risk.



Sophisticated medical devices now have computers embedded within them. This makes the devices vulnerable to hacks/attacks which could allow hackers to:

- Disable systems or key functions.
- Manipulate device configurations/patient treatments.
- Steal patient data.

This is due to the fact that medical device designs focus on features/performance instead of security and that they are designed to operate for decades while software support to fix vulnerabilities is designed to last for years instead of decades which forces device makers to try to support equipment for significantly longer than intended.

To fix this, device makers must design their devices with security in mind to ensure that only authorized users/systems can access/configure them and to allow for OS patches and upgrades as needed. Finally, hospitals need to design their networks to isolate/secure medical systems.

A Consequence of Ineffective Controls

Use of Leaky Legacy API

Breach Impact:

People Impacted: The supplied attendee information from all conference registrants was available to download from the Public Internet by anyone without authentication.

The organizers of the annual hacker conference Blackhat USA used an out of date registration system that included a leaky data interface which allowed anyone on the public internet to access and download attendee information for conference registrants without any restrictions (to prevent a mass download).

One attendee discovered the issue, reported it to the organizers and they were able to fix the issue within 24 hours. However, one would expect organizers of a hacker conference to ensure they are using up to date software to avoid embarrassment by their customers.

A Consequence of Ineffective Controls

Relying on Phone # as Identity

Many applications today authenticate users not with a password but with a PIN sent to their mobile phone. The theory is that since the pin changes each time and users ALWAYS have their phone with them, it is more secure than just a password. The problem is, that when the phone breaks, is lost or stolen, the user has no access to their account. In addition to the above risks, if a hacker wants access to your account badly enough, they can convince your cell carrier to port your phone number to a different phone and redirect the pin texts without your knowledge or approval. There is currently a multimillion dollar lawsuit pending against at&t for porting a customer's phone number a 2nd time in violation of additional security precautions they had agreed to implement to prevent it. This allowed the hacker to steal millions of dollars in bitcoin from the customer. Bottom line, your phone number is only as secure as your phone company makes it!

A Consequence of Ineffective Controls

Phones Vulnerable/Infected When Activated

Users rely on their phones to not only function but to also be free of viruses/vulnerabilities. Unfortunately, security researchers have found that some, mostly inexpensive phones, have been found to have a banking Trojan, adware and other viruses pre-installed on the phones. Such viruses can steal user accounts/passwords and expose private user data to hackers. To minimize the risk users should:

- Purchase phones from larger reputable manufactures/sellers.
- Don't purchase just-released phones wait for reviews instead.
- Install and run anti-Virus software on your phone.

A Consequence of Ineffective Controls

Use of Fibits Exposes Secret Facilities

Breach Impact:

People Impacted: Fitbit user data exposed secret military installations.

Gadgets that can help people track their physical activity and encourage them to exercise more are a good thing! After all, a more physically fit and healthy population lives longer and gets sick less often. Furthermore, a more healthy armed forces is happier and more effective. So why has the military banned the use of fitness trackers and smartphones for active duty personnel? Because their geo-location services are enabled by default and are configured to report soldier movements to a central company server where locations soldiers frequent can be tracked and secret installations identified. Bottom line, no matter how helpful smart devices are, by default they are set up to track your activity and report it to the company who can use it as a revenue source. Bottom line, if you do not wish your activity to be the product sold to companies, be mindful of what you use and what options you disable so as to ensure that data you do not want collected and reported is not.

A Consequence of Ineffective Controls

Not Patching/Protecting Smart Devices

Breach Impact:

People Impacted: Personal info on casino high rollers stolen.

As more and more smart devices are installed on company intranets, hackers are finding that many of these devices are either not maintained properly or are not patchable and are left connected to the regular corporate internal network. The problem is that these devices can still be hacked and used by outside entities as a foothold on the network to scan/attack/steal company data. For example, early in 2018 a casino's high roller customer database was stolen. An examination found that attackers came into the casino network through the smart thermometer in the lobby fish tank! Literally any smart device that is on the network and not properly maintained or secured is vulnerable and makes the entire network vulnerable! Smart devices should preferably be kept on an isolated network and granted access to only they systems they need to talk to and nothing else.

A Consequence of Ineffective Controls

Stolen Data Hidden in Legitimate Traffic

Security researchers have found a new way for hackers to sneak stolen credit card data out of the company network. The hackers have found a way to hide the data as a part of legitimate internet traffic such as DNS. Since DNS traffic is normal and necessary, many companies do not block it or scan it. This allows the data to be sent back to the hackers under the company's nose. To catch this, companies need to inspect outgoing network traffic to detect:

- Suspicious data being sent.
- Occurrences of unusually high traffic.
- Larger than expected packets.
- Machines on the network behaving suspiciously.

A Consequence of Ineffective Controls

Hackers Compromise Anti-Virus Software

Breach Impact:

People Impacted: 2.3 million PCs had the infected version of Ccleaner installed during the month the infected software was available.

Over a 6 month period, very determined hackers were able to gain control of key systems on the virus cleaning software CCleaner network and eventually replace the software available for download with an infected version. It then took computer researchers another month to detect the hack by which time 2.3 million downloads had occurred. Fortunately, the virus was relatively easy to remove from systems once found. While this type of attack (software supply chain) is very difficult, rare and is not something normal users can defend against, software manufacturers users rely upon must do more to secure their systems and networks to prevent such attacks!

A Consequence of Ineffective Controls

Brute Force Password Guessing

When hackers obtain usernames and passwords for attractive targets, they try to sell those credentials to others, often on the dark web, so that they can make quick money off of the information they have obtained. Security researchers are aware of this and monitor the dark web to determine what has been compromised and work with impacted to organizations to fix the issue. Over the summer, a security researcher found that a critical airport account was compromised and available for sale on the dark web for $10. For the price of a movie ticket, a hacker can gain access to "systems linked to security and building automation systems." In this particular case, the researchers believe that the password was gained through guessing all possible password combinations (through automation) until they were able to log in. But the password could just as easily been obtained through phishing scams as well. Fortunately, in this case the airport was notified and was able to reset the impacted account password. However, long term, the airport needs to look at moving to two-factor authentication and other controls that would have blocked this attack before it was successful.

A Consequence of Ineffective Controls

Believing a System Is Unhackable

Apple's servers were widely believed to be unhackable. Unfortunately for them, a 15 year old Apple fan in Australia did not believe the hype. He was able to successfully hack into an Apple server, gain access to authentication keys (like a password that is usually kept very secure) and download 90GB of Apple data undetected during the year he had access. Fortunately for Apple, the now 16 year old bragged about his accomplishment on the Internet and Apple found out. They were able to find signs of the intrusion and track them back to a MacBook via its serial number which allowed authorities to raid the teen's home, find the computer and arrest him. In order for companies to have a chance at detecting hacks, they must monitor their networks for suspicious/unauthorized activity and review their systems to see if there are signs of tampering. Stories like this should not occur as it erodes public confidence in them.

Avoid Becoming

A Consequence of Ineffective Controls!

- Don't respond to suspicious e-mails or click on any links within the e-mail.
- Always run up to date anti-Virus.
- Patches for computers, phones and smart devices should be applied shortly after release.
- Use complex passwords both at home and work.
- NEVER share your password with anyone, including support personnel.
- NEVER walk away from an unlocked computer.
- NEVER leave an active (logged in) web session on a shared computer.