2017 Data Breach Digest: December update

Cloud Storming: Forecasting whether systems are in the area

verizon✓

Although cloud-related digital forensics isn't new, one of the challenges we've faced over the years is getting to the evidence in a timely manner at third-party cloud-hosting facilities. Businesses utilizing third-party cloud storage (data centers) are often not aware of the challenges and hurdles that can arise and delay the investigative response efforts.

Configuration Exploitation

the Acumulus Datum

CE-4: Cloud Storming

Don't let the Acumulus Datum ammass your information!

Cloud Storming strikes against offsite services and storage

What can you do?

- ✓ Use $+r0^g passwords and change them regularly
- ✓ Use two-factor authentication for access
- ✓ Keep firewall enabled and updated

Some of the more frequent challenges we face when conducting an investigation involving evidence in a third-party cloud storage facility are:

Locating systems and data.

You should be able to locate systems, memory, logs, and data, as well as the data center(s). Knowing where your data is stored can significantly reduce the time required to get investigative responders in a position to collect and preserve evidentiary data.

Gaining physical access

Is physical access to the data at the third-party data center available for evidence collection or will remote access be the only option? Understanding and testing the access and forensic imaging process ahead of time helps prevent delays in acquisition of the data for analysis.

If a "live" image must be made of the system, can investigative responders physically access the systems in the third-party data center? Working through authorization during an ongoing cybersecurity incident introduces unnecessary delay.

Finding a space for forensic data

If access is possible, can an image of the system/data be exported to a network share or storage device at the third-party data center? If the investigation requires imaging a large system, possibly with a network attached storage (NAS) device, finding a place on the network for the forensically acquired information can sometimes be a challenge.

Having to rely on written agreements

Can you rely on written agreements as proof that you will be allowed to gather the needed evidence and information – systems, memory, logs, and data – in the event of a cybersecurity incident?

Some of these challenges were exemplified in the 2017 Data Breach Digest (DBD) "Cloud Storming – the Acumulus Datum."

“Cloud Storming – the Acumulus Datum” describes a cloud-based digital forensics investigation situation where the victim organization received customer complaints regarding its e-commerce website. Its customers’ first attempts at payment initially failed; however, upon second attempt, they would go through. An inspection of the web page found it to be fake! The victim organization quickly took it offline.

It turns out, a low cost cloud service provider hosted the data halfway across the globe – fortunately we had investigative responders nearby. After finally getting to the data, we were able to determine the fake payment page was coded to upload credit card data in real-time to an external IP address and the second payment attempt processed the data legitimately. The story ended up having a happy ending as the investigation revealed a flaw in the threat actor’s code and no data was actually exfiltrated.

With the challenges highlighted in the Acumulus Datum scenario, and those mentioned previously, the varied and unpredictable nature of these types of cybersecurity incidents require a robust set of options to prevent and respond to cloud-based threats. In terms of recommendations, or more specifically countermeasures, based on our experience, we can provide several “prevention and mitigation” and “response and investigation” of these to tackle the challenges posed by cloud security related data breaches.

What is the cloud?

The National Institute of Standards and Technology (NIST) defines “cloud computing” as:

“… a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction …” [1]

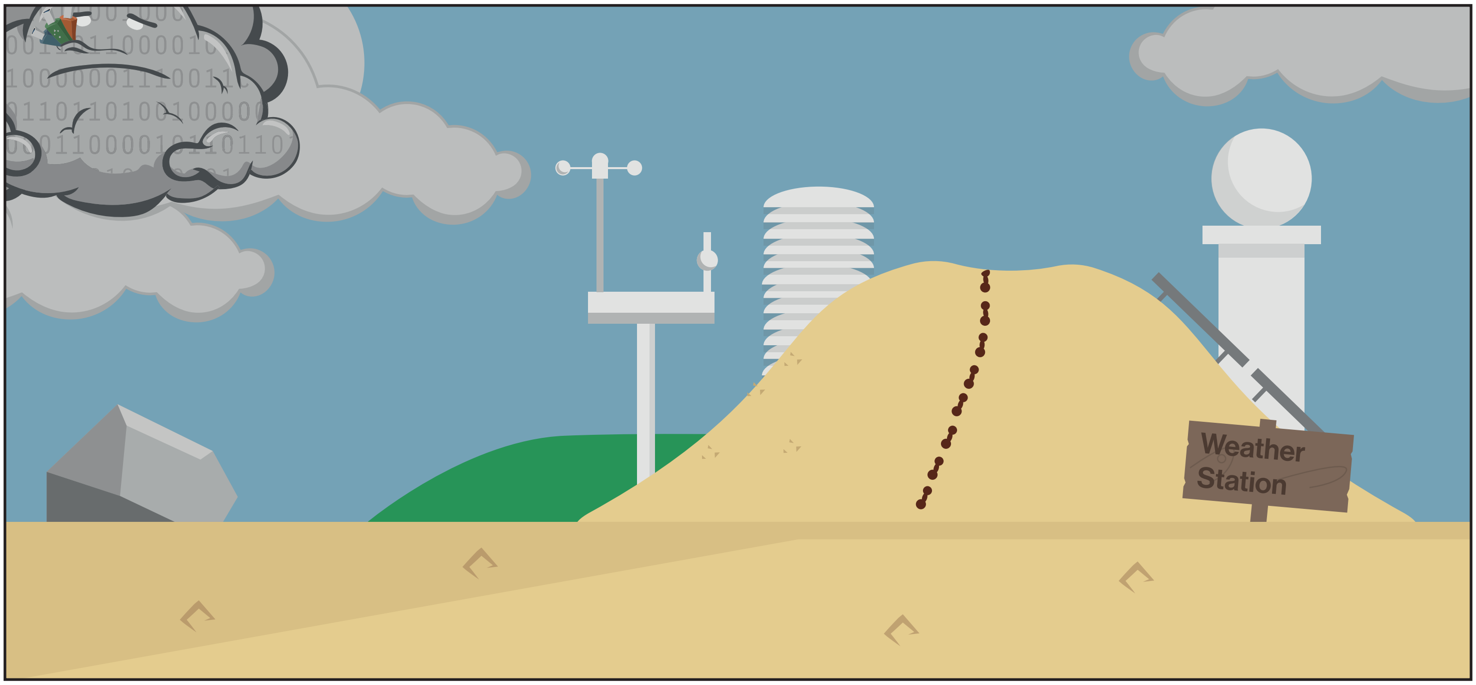
Simply put, it’s putting your data on someone else’s systems.

These “someone else’s systems” are known as cloud service providers, which typically offer services in three categories:

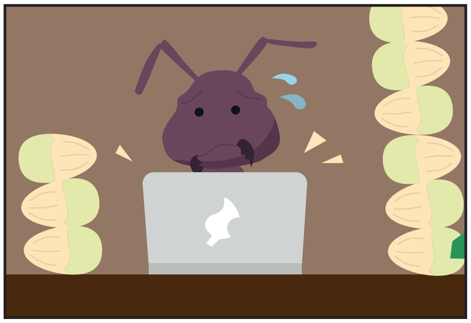
- Infrastructure-as-a-Service (IaaS). Providers manage networking, hardware, and virtualization; the customer manages the software and data
- Platform-as-a-Service (PaaS). Providers manage networking, hardware, virtualization, and operating systems; the customer still manages the data and applications
- Software-as-a-Service (SaaS). Providers manage it all

Regardless of the type of cloud service provider you choose, be familiar with the contract and, in particular, who is responsible for what in terms of cybersecurity. Should a cybersecurity incident occur, you should also know how you can get to your data and logging in a timely manner.

[1] https://csrc.nist.gov/publications/detail/sp/800-145/final

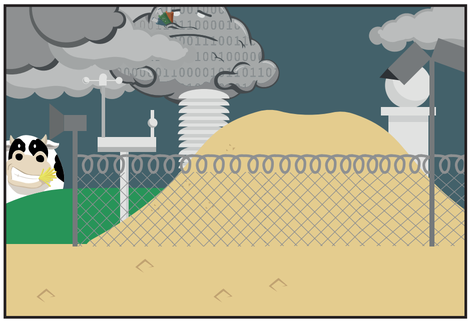


Prevention and mitigation



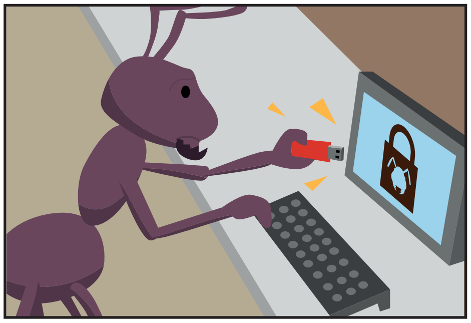
Know where your data is

Discovery is complicated when third parties host data. One of these challenges is not only knowing where your data is, but knowing where your critical data resides. Current, regular and accurate data and asset management through tracking and accountability enhances the speed and efficiency of locating and accessing the correct information during a cybersecurity incident.



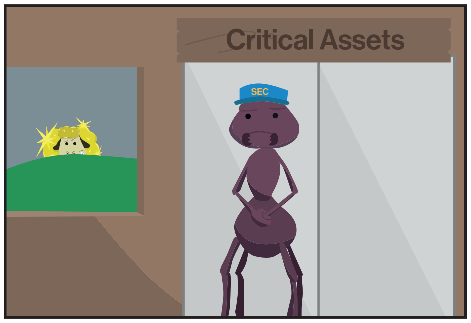
Use a seasoned service provider

Use cloud hosting partners mature in data privacy and security. Even though they may be mature, still periodically assess and evaluate your cloud vendor. Ask to review periodic vulnerability security scanning and penetration testing results to help evaluate whether appropriate layers of cyber, personnel and physical security are in place. Verify that the company meets or exceeds ISO/IEC 27001: Information Security Management Systems (ISMS) – Requirements and ISO/IEC 27002: Code of Practice for Information Security Controls.



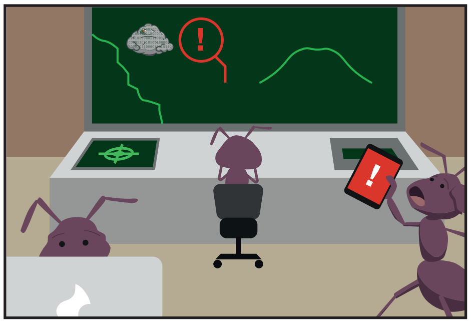
Authenticate using multiple factors

At a minimum, implement two-factor authentication for access to all critical systems. Multi-factor authentication provides additional cybersecurity through multiple layers. It consists of three types of authentication: something you know (password), something you have (token) and something you are (biometric). The more layers of protection that are in place, the better your protection from unauthorized users attempting to gain access to critical systems and data.



Limit access to critical assets

In addition to using multi-factor authentication, restrict direct access to trusted users and IP addresses only. Assign (and review) user accounts by following the "least privilege" principle of cybersecurity. This means granting only the level of authorization necessary to complete the tasks required on the network for that user. The fewer high-level privileged accounts an intruder can potentially compromise translates to a lower probability of those accounts being used in an unauthorized manner.



Make log data impactful

Enable and centralize logging in a way that is easy for investigative responders to access during a cybersecurity incident, to help them get the answers as quickly as possible.

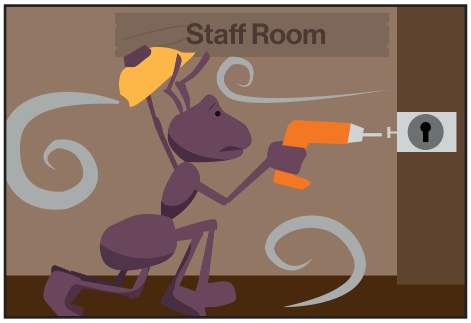
Use packet capture or endpoint detection and response (EDR) technology to enhance network and system logging. EDR addresses the need for continuous monitoring and response to advanced threats. The analytics tools EDR uses to process the data collected from the endpoints can reduce the time the investigative responders need to zero in on an unauthorized user's activities across a network.

Response and investigation

Leverage incident response playbooks

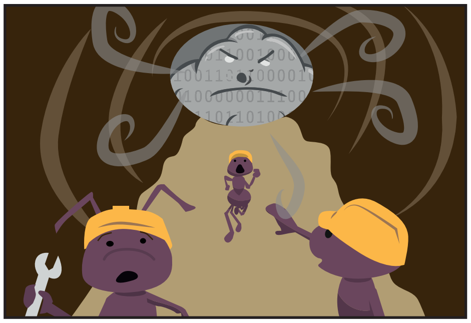
In addition to an incident response (IR) plan, create IR playbooks for the most relevant data breach and other cybersecurity incidents for your industry and organization. As with the IR plan, develop and implement IR playbooks that incorporate industry best practices, collection methods and processes for evidence located at third-party cloud hosting facilities.

Frequently test and update the IR playbooks to provide reliable communication and effective coordination with IR stakeholders and other third-party vendors, including cloud hosting facilities.



Change admin passwords immediately

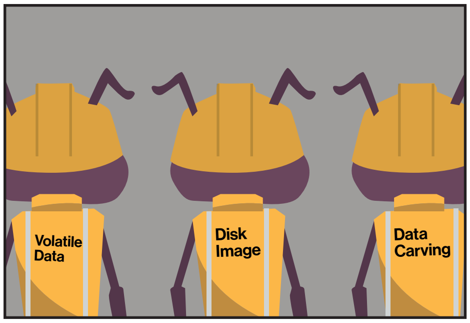
No one enjoys the inconvenience necessitated by a password changing party, but it is a necessary process for in-scope user accounts when responding to a data breach or cybersecurity incident. Local and network admin accounts are favorite targets of intruders and should be the first passwords changed in the event of a breach.



Get to the data quickly

Streamline data center required ticketing systems to enable collection of evidence. Data center ticketing systems are generally not designed to expedite the forensic imaging of data from the systems under their care and control.

Your data center should be aware that in the event of a cybersecurity incident affecting your data at its location, you'll be requesting its cooperation. This cooperation is integral to getting to your data so that investigative responders can conduct their investigation as quickly and efficiently as possible.



Be flexible with data collection options

Know ahead of time which methods are available to collect and preserve your data for a cybersecurity investigation. Confirm and test options to acquire volatile data, physical memory dumps, system disk images and any log data as expeditiously as possible.

Not all data centers are aware that digital forensic investigations require evidence collection using industry best practices to preserve data in the best possible original state. Be ready to "carve out" data from multi-tenant cloud-based environments.

The way forward

The countermeasures above are some of the actions we recommend based on what we've experienced over the years. These actions should help reduce your incident response time, give you one leg up on knocking out your digital forensics investigation and, in doing so, help you resolve cybersecurity incidents in an efficient and timely manner.

Would you like to know more about data breaches?

2017 Data Breach Investigations Report

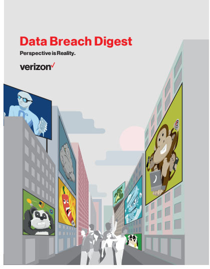
Get the 2017 Data Breach Investigations Report (DBIR). It's our foremost publication on cybersecurity, and one of the industry's most respected sources of information.

http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

2017 Data Breach Digest

Read the Data Breach Digest (DBD) for the story of Verizon's most intriguing cybercrime investigations. Learn about the attackers' tactics, the victims' mistakes and the scramble to limit the damage.

http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017/



verizonenterprise.com