
# EXECUTIVE GUIDE TO THE MOVIELABS ENHANCED CONTENT PROTECTION FOR PRODUCTION (ECPP)

VERSION 1.0

Motion Picture Laboratories December 7, 2021

# Contents

# 1 Introduction

This document provides an introduction and guide to using the more technical and extensive MovieLabs Enhanced Content Protection for Production (ECPP) Recommended Practices.

The transition to production in the cloud is challenging the perimeter security models that have been the foundation of on-premises security. Once cloud services of any form are introduced, the perimeter security model breaks down because of the very nature of cloud services – they are not controlled from the ground up by the user. You can't airgap the cloud.

The MovieLabs ECPP seeks to provide a series of recommended practices to provide guidance in creating and managing cloud security. These recommended practices are not intended to be static, but rather to evolve as the available technology evolves. Although the applicability of recommended practices may vary by situation, MovieLabs recognizes that most of these recommended practices will have broad and strong studio-wide support in most contexts involving the use of cloud resources for the production of motion picture and television content. Each studio will determine individually which practices are required of their suppliers. Those providing production servers and technology should consult with individual studios to determine which recommended practices are required.

This explanatory summary is aimed at:

- Those at production services vendors who are responsible for the operation of the company.
- Those at providers of XaaS[1] services used by production services vendors who are responsible for the product planning, development and implementation.
- Those in studios, productions, and others who are responsible for purchasing and using those services.

Unlike the ECPP document, this document does not require knowledge of cloud or cybersecurity technology. It does not include security methods or references to security tools offered by the cloud providers.

In this document, the term *production* is used, as is the common usage of the industry, to mean either:

- The process of the creation of TV and motion picture content including pre-production, principal photography, VFX, post-production, sound, mastering, etc.

or

- The entity, infrastructure, and people responsible for producing the content.

## 1.1 ECPP Scope

The ECPP document offers security recommended practices for the use of public cloud[2] resources either as an extension of on-premises infrastructure or as the sole infrastructure of motion picture and

[1] XaaS is short for Everything-as-a-Service and sometimes Anything-as-a-Service.

[2] Meaning a cloud infrastructure available to the general public.

television content development, production, and post-production. They apply to use cases where the vendor is in control of the configuration of the cloud infrastructure and security within the boundaries of customer responsibility as described in the cloud provider's shared responsibility model and the users are their employees or contractors.

The ECPP document limits itself to covering only the "cloud deltas" or practices that are new or significantly different for cloud. It does not include practices that should already be in place for productions that use local and on-site infrastructure. Therefore, general IT and network security are out of scope, as are remote work, software development, human resources, site security, and processes for security management. These are all handled in other, well-documented industry practices and are not issues specific to cloud.

## 1.2 Why ECPP is important to you

There are several reasons why you might wish to follow the ECPP recommended practices.

1. Your customers may require it.
    - The ECPP document is not a set of requirements, but it may feature in the security requirements of studios and others contracting production services.
2. You've discovered that cloud security is complex.
    - ECPP can be your guide in configuring cloud security because, without a guide, it can be difficult to know where to start.
3. You've determined that a breach could cost your business revenue and damage its reputation.
    - Nobody can assure you that your system is completely secure, but the ECPP recommended practices are designed to help you create resiliency and build a plan to respond to an incident and recover afterwards.

## 1.3 Categorization of recommended practices

Some ECPP recommended practices are labelled **[baseline]**. These are the "top five" recommended practices (RP) and the ones that should be addressed immediately.

Some of the RPs include measures labelled 'foundational' which means a security measure that should already be part of the security of on-premises infrastructure. Foundational measures are necessary to implement the recommended practice.

## 1.4 Terms and definitions

Some terms are fundamental to the discussion and need to be defined to avoid confusion. We use the NIST[3] definitions of cloud computing terms. It is not important that you remember these definitions but if you need them as a reference, they are listed in Appendix A.

One term though should be understood, ECPP is about security and references external documents that use cybersecurity vocabulary. Therefore:

[3] National Institute of Standards and Technology, https://www.nist.gov/

An *Asset* is any data, device, or other component (hardware or software) that supports information-related activities.

*Media Asset* is the term we use to mean any data and metadata that is part of the process of media creation including image data, sound data, and metadata. Within media production these are usually referred to simply as *assets*.

The other term you should understand is *vulnerability*. This is a defect or weakness in a particular system, module, or component that leaves it open to being compromised due to attack.

# 2 The Cybersecurity Landscape

We cannot consider the security of media production in isolation from the wider cybersecurity landscape. Our industry does not get a pass because it does not handle financial or healthcare data, and like those industries threats to media production come from professional criminals as well as amateurs. In this section we look briefly at the wider issue of information security.

## 2.1 The threats

Top of the list of threats are unauthorized access to data and business disruption.

- Examples of unauthorized data access include access to media assets, to backend system data including personnel data, and to proprietary software.
- Examples of business disruption include network DDoS (distributed denial of service) attacks and ransomware which is itself a denial-of-service attack.

Well-known attacks have included both elements – exfiltration of data together with the deployment of ransomware either for the attackers' own reasons or for a "double" ransom demand – the payment to stop the data being published and to unlock the data.

## 2.2 The threat actors

The question is, who are the threat actors? Verizon's 2021 Data Breach Investigations Report (DBIR) identifies the top threat actor varieties in 2,277 breaches, showing that approximately 80% of breaches are by organized crime but, leaving aside a small percentage to nation state actors, most of the rest are employees and unaffiliated actors.

Whether or not organized crime is such a significant threat in our industry, we do know that theft of pre-release content and ransomware are both sources of income for criminals.

A small vendor that is victim of a ransomware attack may find the ransom is disproportionate to the vendor's revenue if the attacker is looking at the bigger picture – the ransomed data is part of a very expensive production.

We cannot afford to underestimate the threat actors. They are getting much more sophisticated, and they too have an extensive set of cloud offerings to draw upon. We are not talking about threat actors with the superhuman skills who leap over the 20' chain link fence you just erected, we are talking about threat actors who are very skilled at sweet-talking you into handing over the keys to the gate.

Risk is assessed in terms of possible damage, the likelihood of a breach or incident, and the cost of remediation. We do not assess risk in terms of the motivation of the attacker. The question "why would anyone do that?" is best left unasked and unanswered.

## 2.3 Breaches and incidents

It is worthwhile to understand the nature of breaches and incidents. Those two things are not the same: an *incident* is a security event that compromises the integrity, confidentiality or availability of an information asset and a *breach* is an incident that results in the confirmed disclosure of data to an unauthorized party.

The DBIR reports the follow patterns:

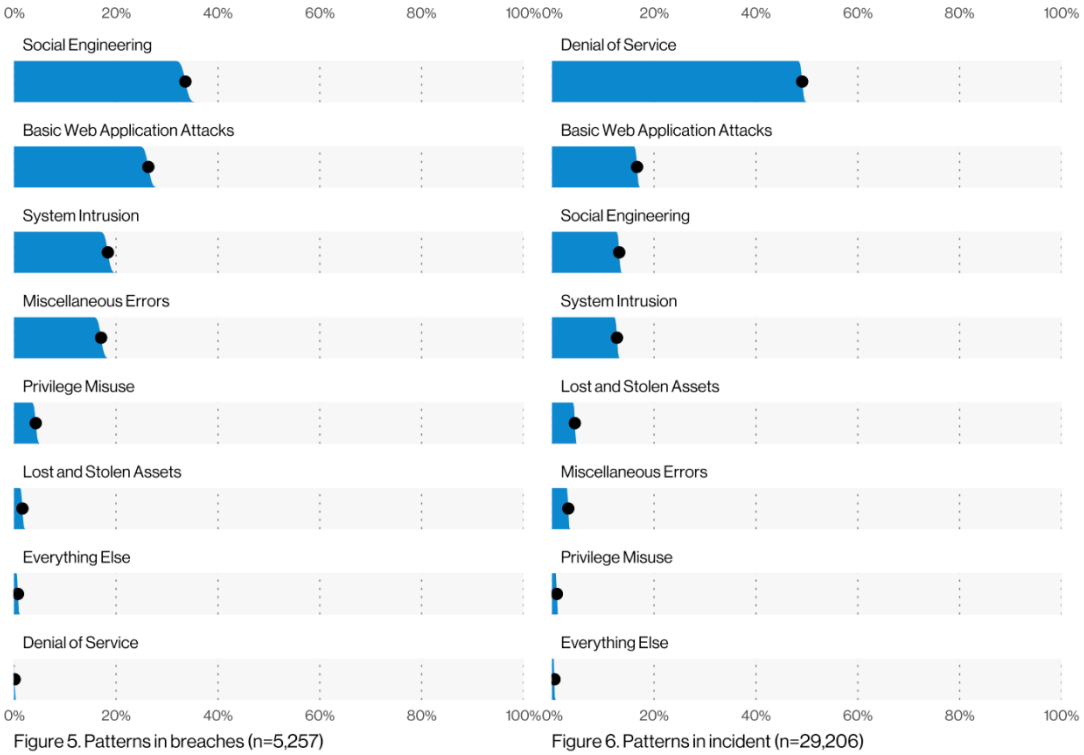


*Figure 2-1 Breach and incident patterns (source: DBIR)*

The DBIR report looked at action varieties, not surprisingly the human element and credential misappropriation are high on the list. Threat actors target human carelessness and human fallibility. Social engineering cannot exist without both being present.

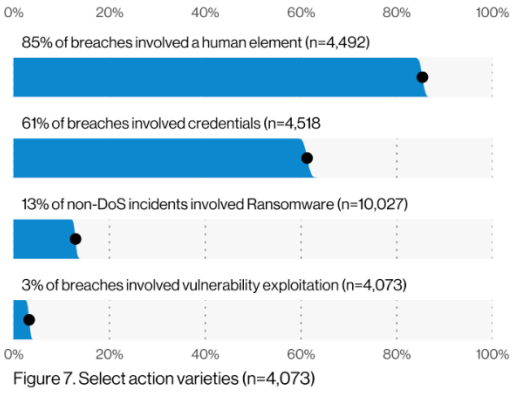


*Figure 2-2 Action varieties are weighted toward the human element (source: DBIR)*

And lastly from the DBIR is this figure:

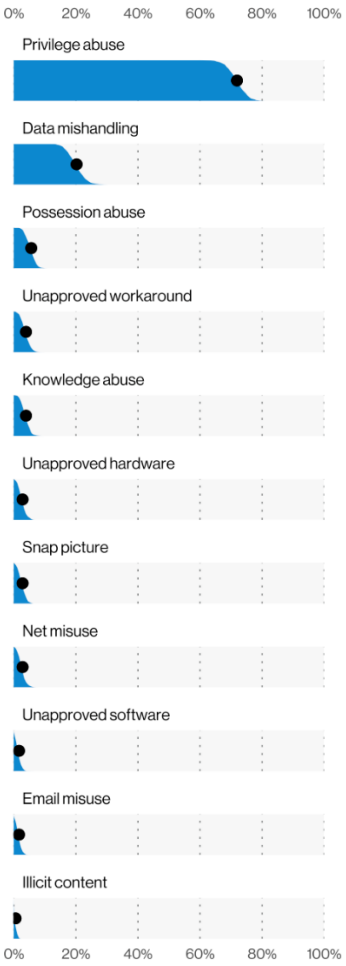


*Figure 2-3 Misuse varieties tilt toward credential based attacks*

This tells that properly training staff in security procedures, phishing and social engineering is critical to the security of your operation. The uninformed is more likely to make mistakes, be phished, etc.

# 3 Security Basics

The place to start planning your security strategy is not at the security dashboard of your cloud services provider. You need a plan and, generally, the methodology to create the plan would not be much different from the plan you had if you secured on-premises infrastructure. Where it will differ is in the tools you will use to go from plan to action.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework assists us in formulating that plan.


*Figure 3-1 NIST Cybersecurity Framework 1.1*

You need to have each one covered – or at the very least examined and a decision taken that it doesn't apply to you (which is, frankly, unlikely).

The five components are:

- **Identify** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

Risk is based on likelihood, for example an attack that uses quantum computing is unlikely, and consequence including how your business, your staff and your customers be affected. If you don't know what you need to defend and what you need to defend it from, you don't have a place to start.

Risk management can be a formal process, the FAIR Institute (https://www.fairinstitute.org/) offers resources for risk management including their publication "Measuring and Managing Information Risk: A FAIR Approach" and there are several accepted frameworks listed in the ECPP document. However, it could also be less formal. The important aspect is that the risk assessment can help make judicious use of the security budget by directing efforts in the best direction.

- **Protect** Develop and implement appropriate safeguards to ensure service delivery. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

Security tools and best practices from the cloud providers are designed to assist you in protecting your use of their services.

- **Detect** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

Probably the most important part of any security system is being able to detect that something is amiss. An intruder can lurk in your network only if you cannot detect they are there. Detecting an intrusion is the first step to doing something about it.

- **Respond** Develop and implement appropriate activities to take action in the event of a detected cybersecurity incident.

This is the plan you have ready for the time that an event is discovered. It is too late to make something up when something happens (that's a bit like waiting until there is a fire before putting up fire exit signs and installing extinguishers).

And you must practice the plan, just like you would have a fire drill. The lessons from practicing should be used to update/improve the incident response plan.

Contacts with law enforcement and cybersecurity incident response specialists such as Mandiant (https://www.fireeye.com/mandiant.html) and CrowdStrike (https://www.crowdstrike.com/) should be established before you need them.

The list of actions you must be prepared to take include:

- Mobilize the incident response team.
- Identify the root cause of the breach and close it.
- Shut down all active intrusions.
- Determine the extent of any breach and loss of data.
- Inventory the state of your systems.
- Notify your clients and law enforcement. Both will want detailed information that you may not have yet.

Regular tabletop exercises to practice your incident response plan are being conducted including the use of security consultants to conduct "war games." The lessons from these exercises should be used to update/improve the incident response plan.

- **Recover** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Your business demands that recovery is swift. For example, in the event of an attack that denies access to data (such as a ransomware attack), what will you do? This should be closely linked to your business continuity plan. That plan should be updated to include recovering cloud resources. Your recovery plan must be able to recover from part of your recovery plan not working.

(An example of this is your recovery plan says if your building falls down, you will rebuild using the same bricks. Your building falls down and you discover that building codes don't allow new buildings made of brick.)

## 3.1 Threat modelling

Threat modeling provides a systematic approach to aid in finding and addressing security issues early in the design process. There are formal threat model frameworks which may be unnecessary for a small vendor with few cloud-based workflows, but some sort of threat model is advised.

Your threat model is a combination of:

1. Risk assessment including a list of what needs protecting and identifying the assets, actors, entry points, components, use cases, and trust levels to be protected and what the threats are.
2. The measures taken (or planned) to mitigate those risks including any controls in place or planned.
3. Reviewing the risk matrix to determine if each threat is adequately mitigated.
4. Guessing. Informed[4] guessing may be good enough provided you consider the components listed above.

A risk matrix looks like this:

| Impact / Likelihood | Negligible | Marginal | Critical | Catastrophic |
|---|---|---|---|---|
| **Certain** | Stubbing toe | | | |
| **Likely** | | Fall | | |
| **Possible** | | | Major car accident | |
| **Unlikely** | | | Aircraft crash | |
| **Rare** | | | | Major tsunami |

*Figure 3-2 Risk Matrix (source: Wikipedia)*

Threat modeling is most effective when done at the workflow level, ensuring that all context is available for assessment.

## 3.2 Authentication

Without effective and robust identity management it is impossible to secure anything from a building to cloud usage.

ECPP recommended practices for authentication reduce the burden on users when it comes to logging in.

Single Sign On (SSO) is an authentication approach where users use a single login for all the systems they use – that's not the same as using the same password for all the systems! SSO is a powerful security tool and one that improves both security and the user experience. It improves security because it lowers the

[4] Uninformed guessing is likely to be counterproductive.

complexity of managing authentication. The use of multiple authentication systems increases the probability of a configuration error and users are more likely to use simpler or same passwords.

## 3.3 The rule of least privilege

Once a user's identity has been authenticated, they must be authorized for each activity they wish to carry out. That is where the principle of least-privilege comes in.

Least privilege means that a user or a process should be granted only those privileges which are essential to perform the intended task and those privileges should last no longer than is required to finish the task.

This is minimizing what is called the "attack surface", the places where the system can be attacked, by reducing the number of ways that sensitive data can be accessed. If an account is compromised, the breach can extend to whatever that user can access.

## 3.4 The fallacy of VPNs

A virtual private network (VPN) extends a private network across the Internet and enables users to send and receive data as securely as if their computing devices were directly connected to the private network. The danger of VPNs is that they create an illusion of security. There is a tendency to trust devices connecting to a network over a VPN as though they were authenticated devices attached to the local network.[5]

## 3.5 Activity monitoring

The standard approach to cybersecurity is to monitor network and system activity for abnormal behavior. This requires an answer to the question "what is abnormal?". Network activity associated with access to cloud resources used in production is likely to be more limited in scope (not volume!) than network traffic on the corporate network.

The fewer things that must be monitored, the clearer the picture. ECPP recommends segregation of production and non-production traffic and isolating systems one from the other.

Networks and systems should be actively monitored using analytic tools coupled to work scheduling management so that normal behavior can be learned. Activity that is not in the normal range should be flagged for further investigation.

## 3.6 Ransomware mitigation

Protecting against ransomware is complex and, if all else fails, will depend on your backup and business continuity strategy. There are several variations of the 3-2-1 backup rule, but they come down to three copies, stored on different devices and storage media, and one backup is kept off-premises. We say that

[5] Trusting devices that connects to a network over a VPN as much as directly attached devices is perfectly reasonable if you are using zero-trust and don't let anything on the network until it has been authenticated.

two copies need to be stored such that files cannot be overwritten. Off-line media is an obvious option, and another would be a backup to a cloud service where files cannot be overwritten.

ECPP recommends reading:

1. *Ransomware Guide* published by the US Cybersecurity and Infrastructure Security Agency (CISA). https://www.cisa.gov/publication/ransomware-guide.
2. *Mitigating malware and ransomware attacks* published by the UK National Cyber Security Centre. https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

## 3.7 Phishing mitigation

Phishing is a type of social engineering where an attacker sends a fraudulent ("spoofed") message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.

Do not make the mistake of seeing phishing only as a way of acquiring user credentials. The best defense against phishing attacks is user education.

Reliable sources of information include:

1. Phishing attacks: defending your organization, UK National Cyber Security Centre. https://www.ncsc.gov.uk/guidance/phishing
2. Avoiding Social Engineering and Phishing Attacks, US Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/tips/st04-014

## 3.8 Audit and assurance assessments

However qualified and skilled the security team members are, it is important to have your security audited by independent assessors. This may be a requirement in business agreements.

An essential component of any security measures taken for on-premises and cloud infrastructure is vulnerability scanning and penetration testing. For the purposes of this section, we will use the term “pen testing” to avoid confusion with the process of vulnerability assessment.[6] (For the avoidance of doubt, we are referring to the process of penetration testing not the tools to perform penetration testing.)

The UK Cyber Security Center defines penetration testing as "*A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might*."[7]

Your report will either give you a clean bill of health, or it will require action. The former is unlikely. Unless you are prepared to fix everything, the next step is risk assessment. The pen test report should help you determine the impact of an attacker exploiting a vulnerability would be and how likely it is to

[6] https://en.wikipedia.org/wiki/Vulnerability_assessment
[7] https://www.ncsc.gov.uk/guidance/penetration-testing

occur (the risk matrix mentioned earlier). This is input to your risk assessment and management process where controls (preventive, detective and corrective) are put in place to mitigate the risks.

The lifetime of a testing report is limited by a change to the tested system or the disclosure of a new vulnerability in any of the software or hardware in the system. To put that another way, pen testing needs to be repeated. Like painting the Golden Gate Bridge, it's a job that is never finished.

Be aware that your cloud provider may have rules about penetration testing your use of its infrastructure.

## 3.9 Keeping up to date on threats

There are multiple sources and feeds of threat information that are relevant to you, and someone must monitor them.

Make sure someone has subscribed to and monitors the CVE list[8] which is the definitive up-to-date repository of known vulnerabilities.

Security responsible vendors, those that understand they must commit fully to securing their products and services, will publish security advisories for their products both on their website and via the CVE list (for example, Teradici's Security Advisories), and will encourage users and researchers to report vulnerabilities either directly or through groups such as HackerOne (for example, see Teradici's Report a vulnerability). HackerOne is an organization of ethical hackers supporting responsible reporting of security vulnerabilities.

Keeping security vulnerabilities confidential is only considered acceptable while no remediation is available, but unresolved vulnerabilities should not be allowed to persist. Not taking every step to remediate a vulnerability as soon as possible is not a responsible action. Software and service vendors must be transparent with their customers.

## 3.10 Management commitment

It is fair to say that in an alarming proportion of breaches, lack of management commitment to security is a contributing or enabling factor.

It is critical that management is fully committed and seen to be fully committed to security and does not make exceptions.

If your star editor complains about two-factor authentication and wants it turned off, the answer is not to turn it off, but it may lie in finding an equally secure but less burdensome way of managing identity such as passwordless authentication[9].

[8] https://cve.mitre.org

[9] One of many passwordless solutions in Microsoft Hello. https://www.microsoft.com/en-us/security/business/identity-access-management/passwordless-authentication

# 4 Shared Responsibility Models

While we are avoiding discussion of cloud provider security tools, it is very important that you understand your cloud provider's shared responsibility model. This describes what aspects of system security your cloud provider is responsible for and which aspects you are responsible for.

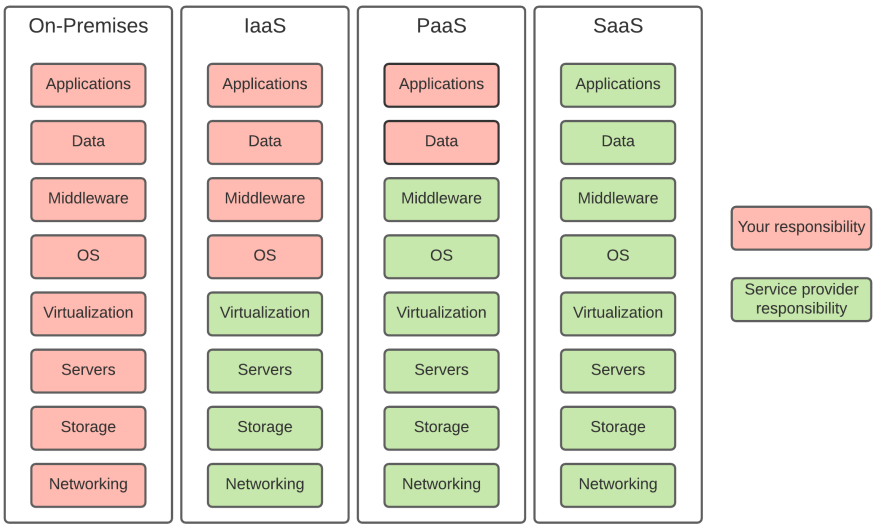


*Figure 4-1 Cloud security shared responsibility*

What we see from this figure is how the security responsibility is divided up for each of the service types we have identified: IaaS, PaaS and SaaS.

Cloud providers publish more detailed shared responsibility models which delineate which part they are responsible for securing and which part their customers are responsible for securing. Here is the AWS diagram:

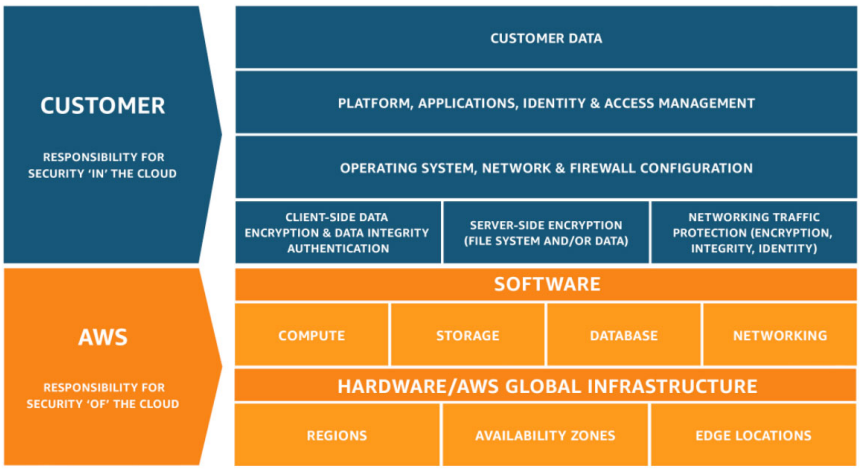


*Figure 4-2 The AWS shared responsibility model*

This division is perfectly understandable, but it does mean that anyone saying “our systems are secure because they are running on <insert name of cloud provider here>” has not grasped the shared responsibility model. Undoubtedly, if your data is stored on Amazon Web Services (AWS), Google Cloud Platform (GCP) or Microsoft Azure, you don’t need to worry about someone stealing the hard drives, but as you can see there is still much to worry about.

# 5 Managing Security

The ECPP document explains the need for a cybersecurity team and creating one will present a challenge to small and, possibly, medium sized vendors and is further confounded by a shortage of talent in cybersecurity.

This document cannot define what is needed by a particular organization because there are too many possible variables.

Here are some basic observations:

- Someone must manage security implications within the organization and that might include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.
- The security team[10] and infrastructure management (IT) team should report independently up to the CEO/president because, in some circumstances, securing a system may mean taking it offline which is the antithesis of the goals of the IT team.
- Security configurations and implementation should be reviewed and tested by someone independent of the person who configured the system[11].
- Security is a highly skilled occupation[12]. If qualified staff cannot be hired for one reason or another, the organization should consider contracting with a company that can manage security appropriately.

In fact, deciding how you create a security team should be the first step because it will help decide which skills you have in house, and the extent to which you need outside security services.

An alternative to creating a security team is to engage the services of a company that specializes in cloud security. The level of engagement can be adjusted according to budget and available in-house skills:

- Risk assessment
- Configuration of cloud security
- Monitoring
- Day-to-day management
- Security assurance
- Breach response planning and table-top/"war game" exercises
- Breach response and recovery

[10] See Appendix B The Security Team

[11] Schneier's law: "Any person can invent a security system so clever that she or he can't think of how to break it". https://www.schneier.com/blog/archives/2011/04/schneiers_law.html

[12] "And because anyone can design a security system that she or he cannot break, evaluating the security credentials of the designer is an essential aspect of evaluating the system's security". ibid

# 6 Conclusion

Cloud security can seem to be like trying to assemble a jigsaw puzzle without the benefit of the picture on the box. However, cloud providers have templates for meeting the security required by various regulations and standards. The ECPP recommended practices suggest, failing a better alternative, using an existing security framework that has comparable, at least in part, security requirements as a starting place.

Beyond that, someone in the organization, or someone hired by the organization, must get down to the technical details of risk assessment, configuration, monitoring and planning the response.

# Appendix A Terms and Definitions

## A.1 The NIST definition of cloud computing

We use these definitions of cloud computing from NIST Special Publication 800-145.

### A.1.1 Essential Characteristics:

| | |
|---|---|
| *On-demand self-service.* | A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider. |
| *Broad network access.* | Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations). |
| *Resource pooling.* | The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth. |
| *Rapid elasticity.* | Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time. |
| *Measured service.* | Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. |

### A.1.2 Service Models:

*Infrastructure as a Service (IaaS).* The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

*Platform as a Service (PaaS).* The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

*Software as a Service (SaaS).* The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings

.

### A.1.3 Deployment Models

*Private cloud.* The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

*Community cloud.* The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

| | |
|---|---|
| *Public cloud.* | The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. |
| *Hybrid cloud.* | The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). |

## A.2 Cybersecurity terms and definitions

*Cybersecurity* is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.[13] Cybersecurity includes application security, information security, network security and operational security.

*Authentication* is the security mechanism used to validate an entity's identity by a trusted authority. The entity might be a user, a service, a device, an application, etc.

*Authorization* is the security mechanism used by a trusted authority to determine whether an entity can perform an action.

An *Asset* is any data, device, or other component (hardware or software) that supports information-related activities. This is the cybersecurity definition of the word *asset,* and that definition is chosen because we use quotations from various cybersecurity documents from outside of media production.

*Media Asset* is the broad term we use to mean any data and metadata that is part of the process of media creation including image data, sound data, and metadata. As noted, we adopt this term to avoid confusion with the cybersecurity meaning of *asset*.

*Content Protection* is the protection of the media assets used in the creation of television and motion picture content.

*Security* is used in this document to mean the application of the discipline of *cybersecurity* to a particular use case such as *content protection*.

A *Security Perimeter* is a cordon around a network infrastructure designed to prevent intrusion and the acts of intruders such as content egress. It is a traditional security mechanism for on-premises infrastructure enforced using firewalls and authorized user access from the outside via a VPN.

A *Vulnerability* is a defect or weakness in a particular system, module, or component that leaves it open to being compromised due to attack, disaster, or other causes.

[13] https://us-cert.cisa.gov/ncas/tips/ST04-001

A *Threat* is any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.

An *Incident* is a security event that compromises the integrity, confidentiality or availability of an information asset.

A *Reportable Incident* is an incident deemed to be significant enough to need to be reported outside of the entity. Reporting includes that required by laws or regulations, and those required contractual by contracts with customers.

*Incident Handling* is the corrective action to address an issue/incidence in violation of security practices and recommended practices.

A *Breach* is an incident that results in the confirmed disclosure—not just exposure—of data to an unauthorized party.

*CVE,* short for *Common Vulnerabilities and Exposures*, is a list of publicly disclosed computer security flaws. Each entry in the list is assigned a CVE ID number. See https://cve.mitre.org/.

# Appendix B The Security Team

In this document we make reference to “the security team”. In a large organization it means this:

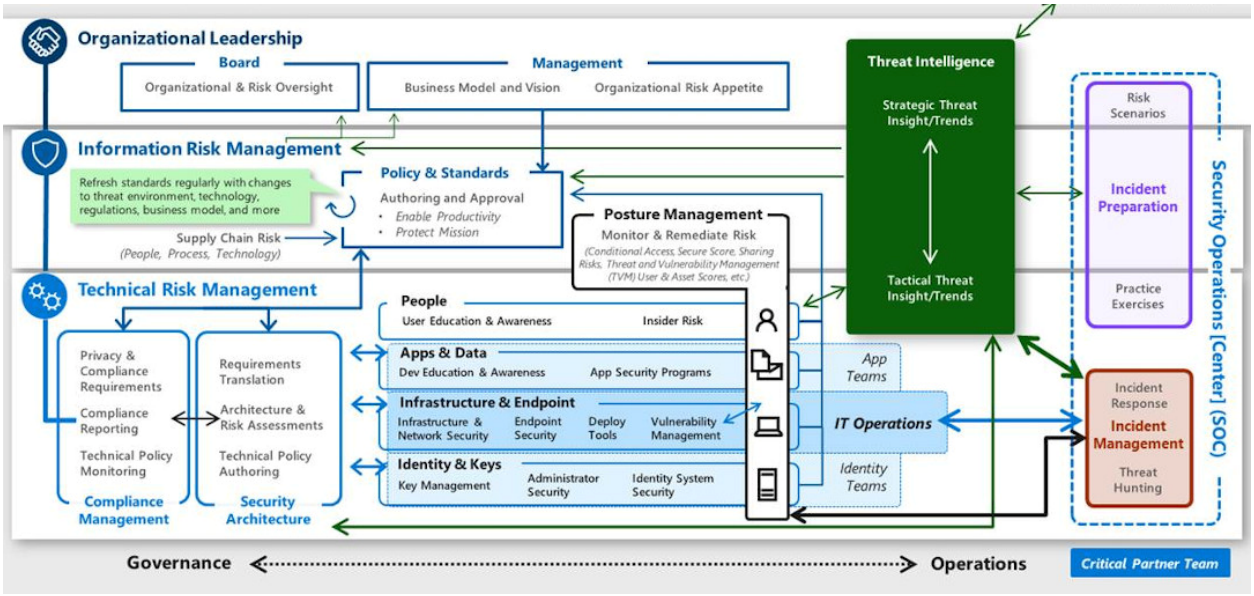


*Figure 6-1 "Each function works as part of a whole security team within the organization, which is part of a larger security community defending against the same adversaries.” Source Microsoft*

In a modest organization, a dedicated security team is out of the question and what is important is that the roles are assigned. The roles are:

| Role | Simple Description |
|---|---|
| Security architecture | You need a security architecture sufficient for your use of cloud services. In the simplest case that is a diagram and a description of the components. Consider it your roadmap. |
| People security | People security protects the organization from inadvertent human mistakes and malicious insider actions. The extent to which you embark on training programs is going to specific to your organization. |
| Application security and DevSecOps | If you develop your own applications, you need to develop them for security. |
| Data security | The main objective for data security team is to provide security protections and monitoring for sensitive data. For many production services providers, this is the goal. |
| Infrastructure and endpoint security | The complexity of securing cloud infrastructure depends on how extensively you are using cloud services. |
| Identity and keys | This role provides authentication and authorization of humans, services, devices, and applications. |

| Role | Simple Description |
|---|---|
| | *This function also plays a significant role in modernizing security by establishing an identity-based perimeter that is a keystone of a zero-trust access control strategy.* |
| Threat intelligence | Security threat intelligence provides context and actionable insights on active attacks and potential threats. This need not be as large a task as it seems, the minimum is monitoring sites where security flaws in the software and the services you use are published. |
| Security operations center (SOC) | A security operations center (SOC) detects, responds to, and remediates active attacks on enterprise assets.<br><br>In a small organization answer these questions: who is going to detect there has been a security incident and who is in charge of doing something about it? |
| Security compliance management | Someone must be responsible for making sure the system has been secured. |
| Policy and standards | Security policies are necessary so that everyone knows what is expected of them. |
| Incident preparation | The primary objective for the incident preparation function is to create the “script” for responding to an incident and ensure the script is practiced and refined. |
| Posture management | Posture management builds on existing functions like vulnerability management and focuses on continuously monitoring and improving the security posture of the organization. |
| Looking forward | Risk constantly changes: new threats and new ways of working. |