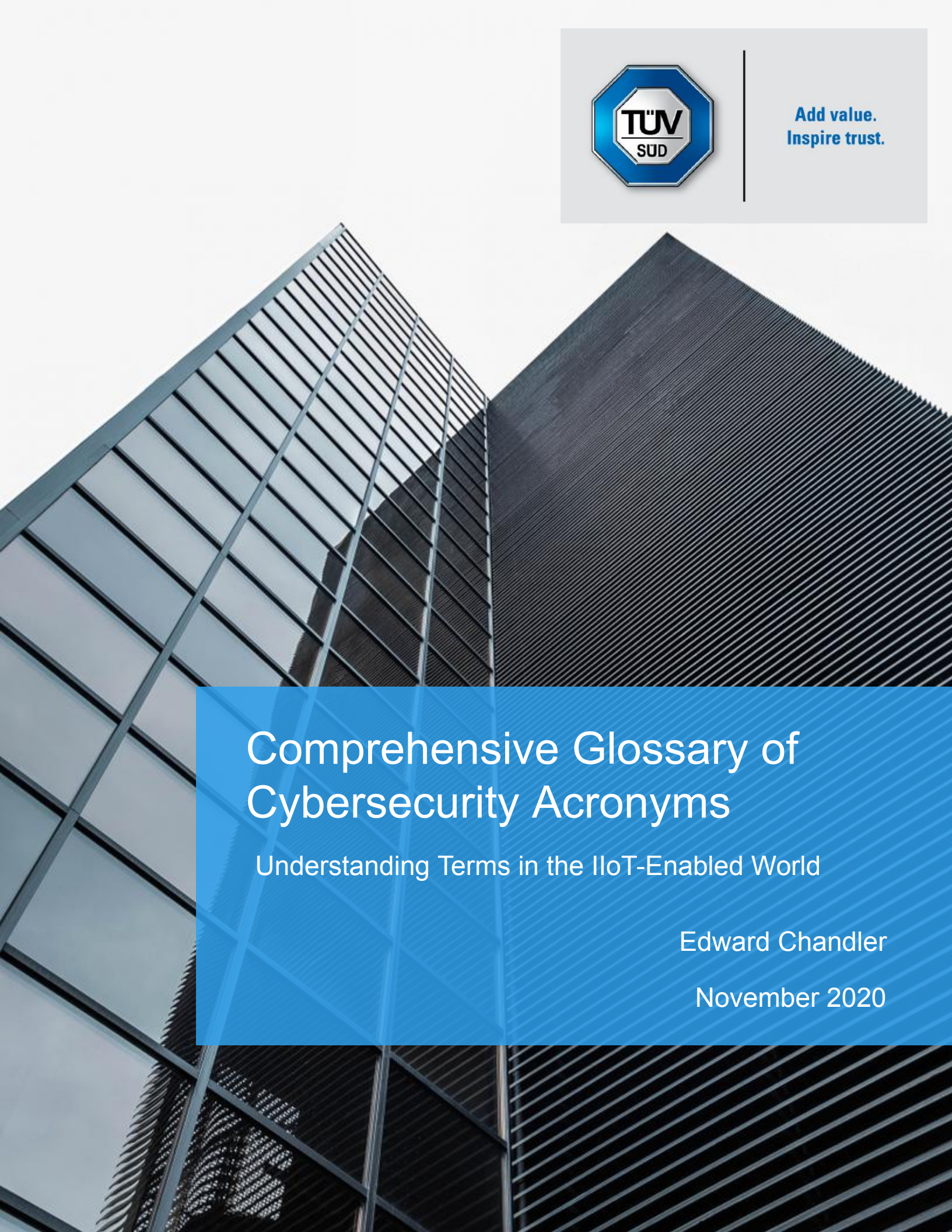


TÜV SÜD

Add value.
Inspire trust.

Comprehensive Glossary of Cybersecurity Acronyms

Understanding Terms in the IIoT-Enabled World

Edward Chandler

November 2020

Why This Was Created and How it Can Help You

The IT and cybersecurity industries are ever changing, and it is a constant learning opportunity.

What I have found throughout my ten years of working in these industries:

- The terms and acronyms usually remain the same
- There are industry-specific terms and definitions I need to bring myself up to speed with based on the organizations I am working with
- Technology is always evolving, and this list can always be updated
- Learning is the greatest form of flattery, and always keeps me on my toes
- IT people are very understanding, and you should never hesitate to ask what they or a term means for clarification

My experience with new companies, industries, and colleagues has led me to compile a list of definitions that people can use to reference or even bring them up to speed with IT security/ cybersecurity lingo and acronyms.

IT and cybersecurity over the years have been in their own worlds separated almost completely from other areas of the organization, or “air gapped” as my IT friends would say. However, this has now changed, and it seems that almost everyone in every part of every company needs to have a basic foundational knowledge of IT and security. Some examples of the two worlds colliding could be: Facilities, Engineering, Operations, Design & Development, and even Executive teams. If you think about it, somebody who was working a press in the 90’s and somebody who is working a press today is a very different concept and most likely uses technologies to actually run and monitor the press.

As any company can tell you, especially those who run ISO management systems, having a common method of communication is key for many reasons, but the most important is to minimize miscommunication. This can significantly improve response, and also minimize the impact of a security incident.

I hope this definitions list will help you and your organization come up to speed, break down those fictional walls, and become more collaborative. This is ever important, especially as methodologies such as Industry 4.0, Smart Facilities, and other ways to create more intelligent environments become even more common.

– Ed Chandler

Table of Contents

1 General IT

IT
Information Technology

- Traditional IT networks that consist of things such as but not limited to Computers, Servers, Printers, and Switches.

OT
Operational Technology

- Non-traditional technologies that focus on the operations of the business. This can include Industrial Control Systems and Machinery.

IoT
Internet of Things

- Non-Traditional IT Devices that may connect to a network, which can include lights, sprinklers, HVAC Systems and more.

IIoT
Industrial Internet of Things

- Non-Traditional Devices that usually is Factory Machinery, Industrial Controls, and the like that connect to a network.

OSI Model

This is a model that helps explain and provides a common criterion for naming communications across an organization. These communications are described as the “7 Layers” which are depicted below.

7 IT Layers

Layer 1
Physical Layer

This layer is just as it sounds. When someone has an issue, it is the first thing the IT person checks. Are all the cables properly connected? Is the power plugged in?

Layer 2
The Data-Link Layer

This layer focuses on node-to-node transfer. There are also two sub layers to this layer. The MAC Layer and the LLC Layer. This is the layer most switches reside.

Layer 3
The Network Layer

This is the layer that focuses on router functionality. It manages things such as packet forwarding.

Layer 4
The Transport Layer

This layer is focused on the management of how data transfers between systems.

Layer 5
The Session Layer

This layer is how two devices on a network can communicate with each other. It will set up the communication, monitor the communication (how long it can take for one system to respond to another system), and the termination of that communication.

Layer 6
The Presentation Layer

Think of this layer as the translator between two organizations. The application layer will take in and put out information in specific formats where the networks layers will be done in a different language.

Layer 7
The Application Layer

This is the layer that most consumers are used to working with as it is the layer they are able to access. This layer is the applications that are web facing. These can include things like websites and mobile applications.

IP Address

Internet Protocol Address

- Unique address for a location of a device; this address is a series of numbers and periods.

MAC Address

Media Access Control Address

- A unique identifier of a type of device, this is a series of numbers, letters and dashes. Each devices is unique, and this is maintained by IEEE (Institute of Electrical and Electronics Engineers).

LLC

Logical Link Control

- This is a sub layer of layer 2. It specifically acts as the link between the MAC Sub Layer and the Network Layer (Layer 3).

LAN

Local Area Network

- Hardwired connected network.

WAN

Wide Area Network

- A non-hardwired connected network, usually through WIFI.

VPN

Virtual Private Network

- Meant to make a computer that is not part of the WAN or LAN become part of the network anywhere in the world. It creates an encrypted tunnel between an offsite computer and a network which is secure. It is highly recommended by most if not all IT departments to utilize a VPN when not on their office network.

SCADA

Supervisory Control and Data Acquisition

- A type of network that is usually associated with utilities such as water and power

NIC

Network Interface Controller

- A device that is used to connect a computer to the network.

Business Continuity Plan

A plan that is developed to ensure if one site goes down, business will not stop. This is required by most security standards and also has its own ISO Certification: ISO 22301.

Hot Spare

- An additional network used where it is actively running and mirroring the network it is meant to replace if one goes down, and have little to no impact to the users.

Warm Spare

- An additional network used where it is occasionally mirrored to minimize the impact experienced by users.

Cold Spare

- An additional network used that will have the necessary things in place to continue business, however, it is rarely backed up and only implemented when necessary.

MSP
Managed Service Provider

- An organization who hosts and manages IT Services for an organization

CoLo
Co-Location

- Shared space used to store networks. The benefit of a site like this is to share equipment, space, power, cooling, and other items.

Cloud
A methodology to store and house networks offsite.

Network Classes

- **Class C**

254 IP Addresses (Most Common Network)

- **Class B**

65,536 IP Addresses

- **Class A**

16,777,216 IP Addresses

DMZ
Demilitarized Zone

- A network that is separated either physically or logically from the trusted corporate network. This usually houses untrusted, and larger devices that are connected to the internet

Air Gap
Two networks that have no connection with each other whatsoever.

Dynamic
Changes all the time. An example would be a Dynamic IP Address

Static
Never changes and remains consistent. An example would be a static IP Address.

ISP
Internet Service Provider

The company who provides bandwidth to an organization. Most common examples would be a telephone or cable provider.

NOC
Network Operations Center

One or more locations that monitors and controls the management of a network.

The Darknet

Hidden networks which are accessed through the internet. Many of these sites on the darknet are used as black markets to sell stolen, sensitive, or illegal content.

Tor
A free open source web browser used to anonymously access webpages, and enables untraceable communication.

2 IT Security

CWE
Common Weakness Enumeration

A maintained list of software and hardware weaknesses.

CVE
Common Vulnerabilities and Exposures

A list of entries each containing an identification number, a description, and at least one public reference.

NVD
National Vulnerability Database

Launched by NIST in 2005. It is a list of commercial software vulnerabilities.

NIST
National Institute of Standards and Technology

An organization fully funded by the US Government, as part of the US Department of commerce, whose mission is to promote innovation and industrial competitiveness.

OWASP
Open Web Application Security Project

A group who works together around Application Security and Launch different projects in the different areas of Application Security. OWASP is most recognized for it's OWASP top 10 List which states the top 10 application security attacks.

ISSA
Information Systems Security Association

A group focused on the improvement of Information Security. This is through sharing valuable information to organizations and security fanatics on ways to protect their networks. Historically this was a USA based organization, however they have launched international operations.

ISACA
Information Systems Audit and Control Association

Similar to ISSA, ISACA is a group focused on the improvement of Information Security through audits and controls. ISACA is also an international organization, however, instead of traditional IT Security topics, they focus on the improvement of security through compliance, audits, and training. ISACA is a very popular organization for training to gain CPE (Continuing Professional Education) credits.

UTM
Unified Threat Management System

- A single appliance that includes a firewall and other IT Security Solutions. These are usually used by smaller companies

DLP
Data Loss Prevention

- A software or hardware solution that locates, monitors, and in some cases prevents the movement of information

Data at Rest

- Data that is not moving across a network

Data in Motion

- Data that is actively moving across a network

Firewall

- A network device used to prevent movement either inward to a network or between networks. There recently have been the concept of a Next Generation Firewall that monitors the traffic bi-directionally

SIEM
Security Information Event Management

- A tool that aggregates and correlates event logs across an organization. This allows security teams to focus on the events that matter and clear out the white noise

WAF
Web Application Firewall

- A network software or hardware tool that is used to monitor not only the security but also the health of a web application

Vulnerability Scanning

- A tool or service used to provide insight into known vulnerabilities. These types of solutions may be used for the internal network, externally facing network, databases, and applications.

Penetration Test

- A service or tool that will look for vulnerabilities and try to exploit those vulnerabilities. To be considered a true penetration test and not a vulnerability assessment there needs to be a human aspect to the test. These can be delivered for the internal network, externally facing network, databases, and applications.

White Box

- Usually a code review. This is used where the tester and scanner have full knowledge and ability to move across a network

Grey Box

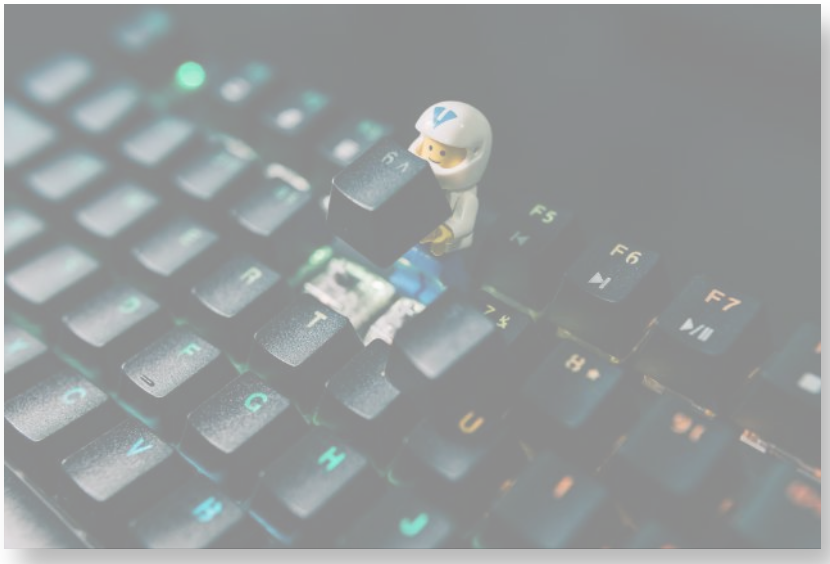
- This is where the tester and scanner have some visibility into the network and what they are supposed to test. It allows them to target the correct or desired assets.

Black Box

- This is where the tester and scanner have no view into the assets that be to be tested and usually must find them on their own. Very much from the mindset of a true hacker.

Red Team Test

- A physical security test where someone tries to physically break into a building and see what they can get away with. This requires a “get out of jail free card,” and the only person who knows that the test is going on, and where it is located is the person who purchased the test. A typical scenario would be someone disguised as a printer repair person who takes a computer and plugs it into the network to see where they can get and if anyone stops them. Think 'Cat Burglar' in the tech world.



NAC
Network Access Control
- A hardware or software solution that only allows trusted and compliant devices on a network. Different NACs use different methodologies such as 802.1X

802.1X
- A compliance standard that is used to only allow, known and or compliant devices on a network

FIM
File Integrity Monitoring
- A software that ensures the integrity of a file

White Hat
- An ethical hacker who breaks code and programs to better the security of them

Black Hat
- An unethical hacker, usually a criminal. This person is trying to break code or programs for malicious purposes such as but not limited to: financial, defacing, or nation state

AppSec
Application Security
- The process of securing applications in development, testing and production stages

DevSecOps
Deveopment Security Operations
- A Combination of Development and Operations Activities in the security world.

IR
Incident Response
- A method that is used to mitigate the response to a security incident. There are also IR Teams who are responsible to respond to the incidents.

Forensics Investigation
- An investigation of a compromised network and/or system. The intent is to stop the 'bleeding,' figure out what has been taken, when it was taken, and how much of it has been taken.

DAST
Dynamic Application Security Testing

- Black-box testing methodology where an application is tested externally, in the way a hacker would.

SAST
Static Application Security Testing

- White-box testing methodology where an application is tested from the inside, usually looking at the code itself.

ISMS
Information Security Management System

- The way an organization manages their sensitive data, this is a way to manage data through policies and procedures. An example of an ISMS is: ISO 27001.

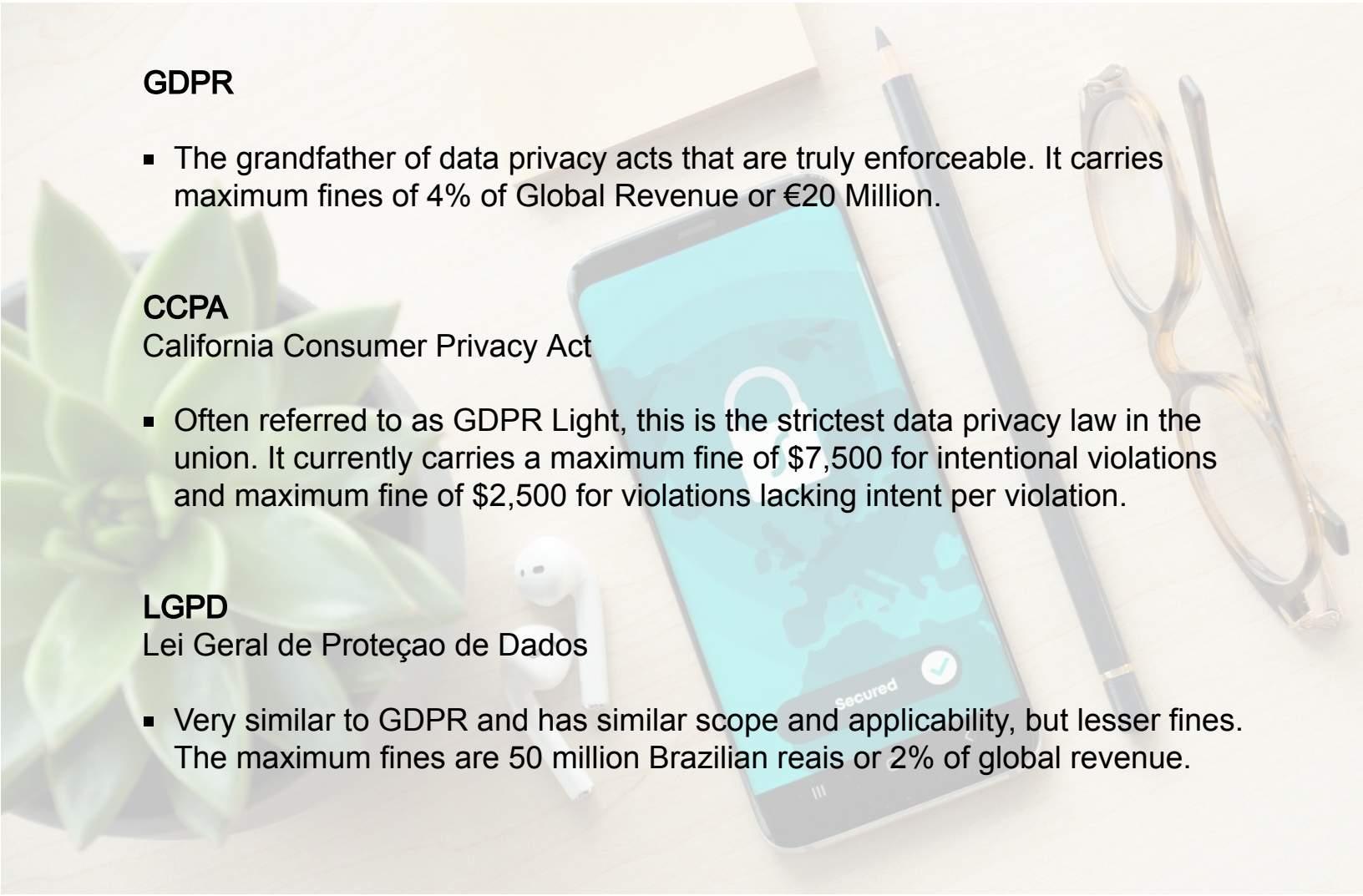
3 Data Privacy

IP (Data Privacy)
Intellectual Property

- Proprietary information that has been developed by an organization. This can be incorporated in products and services. Typically, these are ways organizations differentiate themselves from competitors.

PII
Personal Identifiable Information

- Information about an individual, and can include but is not limited to: name, phone number, email, and address.



GDPR

- The grandfather of data privacy acts that are truly enforceable. It carries maximum fines of 4% of Global Revenue or €20 Million.

CCPA
California Consumer Privacy Act

- Often referred to as GDPR Light, this is the strictest data privacy law in the union. It currently carries a maximum fine of $7,500 for intentional violations and maximum fine of $2,500 for violations lacking intent per violation.

LGPD
Lei Geral de Proteçao de Dados

- Very similar to GDPR and has similar scope and applicability, but lesser fines. The maximum fines are 50 million Brazilian reais or 2% of global revenue.

APA
Australia Privacy Act

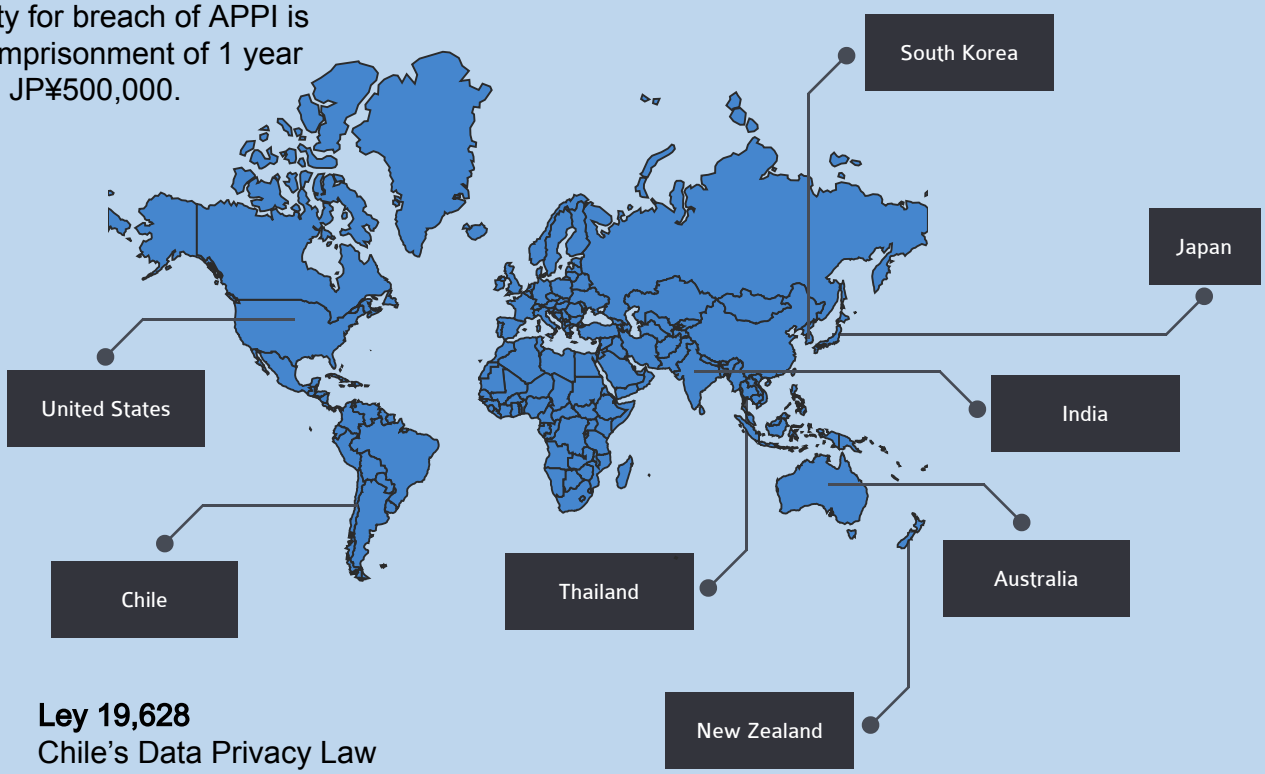
- An organization has 30 days to disclose a breaches that cause “real serious harm” or face fines of up to 1.8 Million AUD.

Japan APPI
Japan's Act of Protection of Personal Information

- Amended to now include both foreign and domestic organizations. The maximum penalty for breach of APPI is currently either imprisonment of 1 year or a fine of up to JP¥500,000.

South Korea PIPA
South Korea Personal Information Protection Act

- The act has a wide array of different penalties depending on the violation. These penalties can include criminal fines, surcharges, and penalties. On the low side it can be ₩ 50 Million, and can get to ₩ 500 Million. For the most serious, these can go up to 3% of a company's global revenue.



PDPA
Thailand Personal Data Protection Act

- In effect as of May 27th, 2020 the max penalty is 5 million, however can also include criminal charges that can be up to 1 year imprisonment and punitive damages can be capped at 2x actual damages.

Ley 19,628
Chile’s Data Privacy Law

- As of March 2020 there is one bill that is in final stages before becoming law, which will be similar in the protections of GDPR. There are also implications for repeat offenders. The minimum fine is 55€ and can get up to 530,000€.

PDPB
India’s Personal Data Protection Bill

- Introduced 12/2019, and expected to pass in 2020. It was modeled after Europe’s GDPR, however it gives much discretion to the central government on how/if to enforce. The fines are similar to GDPR and are expected to be as high as 4% of global revenue.

New Zealand’s 1993 Privacy Act
New Zealand’s Privacy Law

- Some similarities to GDPR, fines are nowhere near as high as GDPR. There is no “Right to Be Forgotten," and the portability of data offshore does is not included for cloud providers.

4 Security Frameworks, and Working Groups

ISO 27000 Series

ISO 27001

- Information Security Management System Certification. An accredited certification for Information Security. Widely required in the manufacturing industry throughout supply chains.

ISO 27002

- Similar to ISO 27001, however this is not a certification. These are guidelines used to improve and stand up information security management. It helps with selection, implementation and management controls taking into the consideration the security environment of the organization.

ISO 27017

- Guidelines for an ISMS specifically for Cloud Services. This is not a certifiable standard and there is no accredited certification.

ISO 27018

- Guidelines for an ISMS specifically for PII (Personal Identifiable Information). This is not a certifiable standard and there is no accredited certification.

ISO 21434

- A standard that is currently under development for the Automotive world, with the intent of being released and required by automotive OEMs in 2023. This standard will take into account both cyber security and functional safety for the developed technology in on-road vehicles.

ISO 22301

- A certifiable standard for business continuity. Widely used in Asia and Europe, this standard is beginning to see much traction in North America

ISO 20000

- A certifiable standard for IT Help Desk operations.

NIST

NIST SP 800-53

- Provides a wide range of security and privacy controls for an organization. This is not an accredited certification, however is one of the most popular information security frameworks in the USA. The intent of this standard is to be used for all US Federal Information Security Systems that do no have national security information.

NIST CSF

- Provides a security framework that is for the security of private sector organizations. The main points of NIST CSF are: Prevent, Detect, and Respond.

COBIT

Control Objectives for Information and Related Technology

- Built and maintained by ISACA. The framework sets guidelines for the management of an organization's network(s). This basis of this framework is: Each process is defined together with Process inputs & outputs, key process activities, process objectives, performance measures, and an elementary maturity model.

OWASP Top 10

- Guidance put together and maintained by OWASP on the top attack categories for Application Security. The current OWASP Top 10 are:
    - Injection
    - Broken Authentication
    - Sensitive Data Exposure
    - XML External Entities (XXE)
    - Broken Access Control
    - Security Misconfigurations
    - Cross Site Scripting (XSS)
    - Insecure Deserialization
    - Using Components with Known Vulnerabilities
    - Insufficient Logging and Monitoring

CIS Top 20

Basic, Foundational and Organizational CIS Controls

CIS

Critical Security Controls aka SANs Top 20

- Initially developed by SANS Institute, however is now managed by CIS as of 2015. This is a best practice guideline developed to increase security within organizations across the world.

Basic CIS Controls

- Inventory and Control of Hardware Assets
- Inventory and Control of Software Assets
- Continuous Vulnerability Management
- Controlled Use of Administrative Privileges
- Secure Configuration for Hardware and software of Mobile Devices, Laptops, Workstations and Servers
- Maintenance, Monitoring, and Analysis of Audit Logs

Foundational CIS Controls

- Email and Web Browser Protections
- Malware Defenses
- Limitation and Control of Network Ports, Protocols and Services
- Data Recovery Capabilities
- Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- Boundary Defense
- Data Protection
- Controlled Access Based on the Need to Know
- Wireless Access Control
- Account Monitoring and Control

Organizational CIS Controls

- Implement a Security Awareness and Training Program
- Application Software Security
- Incident Response and Management
- Penetration Tests and Red Team Exercises

PCI-DSS

Payment Card Industry Data Security Standard

- Developed and maintained by the PCI-SSC (Payment Card Industry Security Standards Council), to standardize the security requirements for all major card brands across the USA. Commonly mistaken as law, this is actually a contractual obligation between a merchant and their processor. There are 12 main requirements, however there are over 300+ sub requirements for an organization to follow

HIPAA

Health Insurance Portability and Accountability Act

- Enacted and signed in 1996, HIPAA is intended to protect personal identifiable health information which has been given to healthcare providers. This is specifically meant to protect consumers from medical fraud. There are stringent fines, and even something called “The Wall of Shame” which is a list of healthcare providers and Associates who have lost patient information through things such as data breach and neglect to follow basic security protocol. With this act there is a significant emphasis on encryption. There is often a misconception by many organizations who claim HIPAA compliance, and that is only one body can audit for compliance which is OCR (Office for Civil Rights) which is part of DHHS (Department of Health and Human Services).

HITRUST CSF

- Developed by HITRUST Services Inc.(Private Company), this cyber security framework in collaboration with organization in the Healthcare, Technology, and Information Security Industries. HITRUST (Company) claims their CSF is a comprehensive, prescriptive, and certifiable framework.

NERC 1300

- A framework utilized by the critical infrastructure sector to protect SCADA assets. The most recent version of this security standard is called CIP-009-3 (CIP = Critical Infrastructure Protection).

ANSI / ISA 62443

- A series of standards and requirements for organizations who want to sell into the Critical Infrastructure Sector. Parts of this series focus specifically on product where other parts focus on more of a traditional management system.

SOC
System and Organizational Controls

- A security certification which is required to be audited by an organization that is part of AICPA. The people who are the auditors usually have a background in financial audit, and the firms are accounting firms.

SOC 1

- For a service Organization Internal Control over Financial Reporting

SOC 2

- Focuses on auditor testing and results. Specifically, the details of data center certification

SOC 3

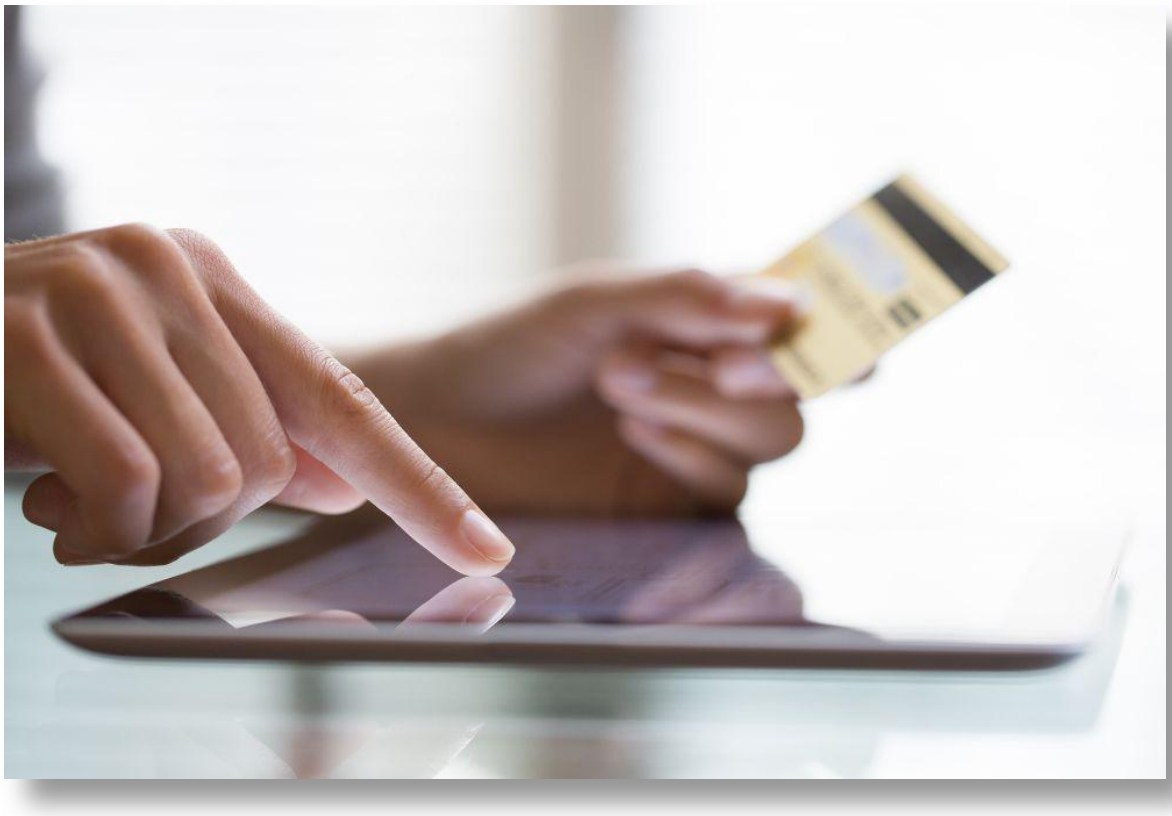
- Is public for public use and is the highest level of achievement for SOC certification. This report includes things such as system descriptions and the auditor's opinions.

AICPA
American Institute of Certified Public Accountants

- A membership organization for certified public accountants

SOX
Sarbanes-Oxley Act

- A law that was enacted on July 30th, 2002. This law's intent is to ensure the protection of financial reporting data.



5 Payment Card Industry

PCI
Payment Card Industry

- The Payment Card Industry has a history of high-profile breaches and organizations being fined large amounts of money due to issues within their PCI-DSS Compliance. Some of these notorious cases that can be found on the web are: TJ Maxx, Target, State of South Carolina, Heartland Payments, and Adobe. Initially each card brand had their own compliance scheme and some schemes conflicted with others, making those schemes highly inefficient and less secure. Due to the amount of breaches occurring, the card brands came together and created PCI-DSS and the PCI-SSC. Other the years there have been many updated versions of PCI-DSS, however one thing remains: There is very little room for interpretation (either you have it in place or you don't), and the standard itself is prescriptive in telling organizations exactly what they need to do to protect card holder data.

PCI-DSS
Payment Card Information Data Security Standard

- Developed and maintained by the PCI-SSC (Payment Card Industry Security Standards Council), to standardize the security requirements for all major card brands across the USA. Commonly mistaken as law, this is actually a contractual obligation between a merchant and their processor. There are 12 main requirements however there are over 300+ sub requirements for an organization to follow

PCI-SSC
Payment Card Information Security Standards Council

- A group of individuals who sit on a committee that determine any changes to PCI-DSS.

ASV
Approved Scanning Vendor

- A vendor that is approved by the PCI-SSC to perform the vulnerability scans that are required quarterly by merchants

- A list of ASV providers can be found **here**.

SAQ
Self-Assessment Questionnaire

- A questionnaire that is required to be filled out by merchants that qualify as Level 3 & Level 4 Merchants, and in some cases by Level 2 Merchants who have an ISA on staff. There are a total of 8 SAQs to choose from and each SAQ is based upon the methods payments are accepted. Below is a brief description of each SAQ, however it is highly recommended that you review each SAQ on the PCI-DSS Website **here**, and/or consult a QSA to ensure the correct form is completed.

SAQ A
- Card-not-present transactions, where a third party handles the CDE of that site. To fill out SAQ A your service provider must be PCI-DSS Compliant

SAQ A-EP
- This again is for ecommerce merchants. When you have outsourced payments completely; however, there is a portion on your website that could potentially impact the security of the transaction.

SAQ B
- Merchants who use the old fashioned imprint machines mostly utilized prior to 2000, and standalone dial up terminals that do not store card holder data.

SAQ B-IP
- Merchants who use standalone dial up PTS Approved terminals that do not store card data.

SAQ C-VT
- Merchants who manually enter each card payment into an online portal hosted by a PCI-DSS validated service provider that does not store any card holder data.

SAQ C
- Merchants whose terminals connect to the internet, but do not store any card holder data.

SAQ P2PE-HW
- Merchants who only use hardware payments that have been reviewed and approved by PCI SSC. These vendors are listed **here**.

SAQ D
- The Grand Daddy of all SAQs. This SAQ has the most requirements for merchants to respond to, and due to the nature of PCI-DSS one requirement failing will make the entire SAQ fail. This is utilized by all payment types that we have not already described. One of the most common automatic requirements for SAQ D is the storage of card holder data. This also must be completed by all service providers that are eligible to complete a Self-Assessment-Questionnaire.

QSA
Qualified Security Assessor

- An accredited individual who performs assessments against PCI-DSS.
- A list of firms who can provide assessments by QSAs can be found **here**.

ISA
Internal Security Assessors

- Level 2 merchants have the option to complete the correct SAQ by an Internal Security Assessor. These assessors must go through regular training to maintain their ability to perform these audits. They are also required to be on staff at a company. Most Level 2's typically lean towards doing a Level 1 for cost and liability purposes.

PA-DSS
Payment Application Data Security Standard

- A standard put in place to minimize the risk of utilizing Payment Applications. This standard will be retired by late 2022.

PCI-S3
Payment Card Industry Software Security Standard

- This is the standard that will take over PA-DSS after it sunsets in 2022.

CDE
Card Data Environment

- The environment in which card data is: processed, stored, or transmitted.

The Twelve Requirements

In PCI-DSS, there are 12 main requirements that a merchant must follow for validation. Seems simple, right? Not so much… There are only 12 requirements, however, there are 300+ sub-requirements that a merchant may need to follow depending on their merchant level and their methods of accepting payments.

The number one way a merchant fails a PCI-DSS Assessment is by not having proper policies and procedures in place.

Requirement 1
- Protect your systems with firewalls

Requirement 2
- Configure passwords and settings

Requirement 3
- Protect stored cardholder data

Requirement 4
- Encrypt transmission of cardholder data across open, public networks

Requirement 5
- Use and regularly update anti-virus software

Requirement 6
- Regularly update and patch systems

Requirement 7
- Restrict access to cardholder data to business need-to-know

Requirement 8
- Assign a unique ID to each person with computer access

Requirement 9
- Restrict physical access to workplace and cardholder data

Requirement 10
- Implement logging and log management

Requirement 11
- Conduct vulnerability scans and penetration tests

Requirement 12
- Documentation and risk assessments

Acquiring Bank

- The source of settlements, disputes, and more.

Processor

- The portion that is very labor intensive such as authorization, settlements, data transmission, security and even connections to the payment networks.

Merchant

- This is the organization who has decided to accept payment cards for their good or services. There is a very common misconception in the Payment Card Industry, and that is: It is law to follow PCI-DSS. This is not the case; however, it is a contractual obligation from your processor/acquiring bank that must be followed to accept card payments. Those merchants who choose not to follow PCI-DSS but still to accept payment cards are liable for: fines, withholding of funds, and shutting down their ability to accept cards. If a breach occurs, those fines become much higher and can be incredibly damaging to a business. Also, please note if a breach does occur, that merchant will automatically become a Level 1 merchant until a later date.

Level 1

- Over 6 million transactions annually.
- The requirement for this level is that you complete a yearly assessment with a QSA, and receive a compliant RoC.

Level 2

- Between 1-6 million transactions annually.
- The requirement for this level is that you complete either a yearly assessment with a QSA and receive a compliant RoC, or you complete a compliant yearly SAQ with an ISA and provide the attestation to the bank.

Level 3

- Between 20,000-1 million transactions annually.
- This requires a yearly self-attestation of compliance with the correct SAQ completed. There is no requirement for an accredited person to complete this SAQ and is usually completed by someone on IT staff.

Level 4

- Under 20,000 transactions annually.
- This requires a yearly self-attestation of compliance with the correct SAQ completed. There is no requirement for an accredited person to complete this SAQ and it usually completed by someone on IT staff, 3rd party IT staff, or the owner of the company.

CVV
Card Verification Value

- This is a verification code that is the 3 digit code on the back of your card, or with American express it is a 4 digit code on the from of your card. For PIC-DSS there is no reason this number should ever be stored for any reason,

Track Data

- The information on a payment card about the person who's card it is. This allows the transfer of money from one account to another.

PTS
Pin Transaction Security

- This is fairly new within the United States, however, was used in Europe for many years prior. The new chip on people's credit cards which eliminates the need of a track data swipe. This technology became very prevalent around 2015

Service Provider

- An organization who to is a third part provider in the Payment Card Industry Market. This service provider can, host, process, store, transmit data on someone's behalf. If the service provider utilizes technologies they have built they may be required to abide by PCI-DSS and that the devices they create certified to PA-DSS

P2PE
Point to Point Encryption

- This is a technology used to process credit cards. It allows many merchants who are utilizing other methods of payment to only have a subset of the requirements apply to them, which is why the PCI-SSC created SAQ P2PE-HW. While this sounds appetizing, the path to becoming a solution that will eliminate the requirements of SAQs is tough, long, drawn-out and expensive. A list of the approved P2PE vendors are listed **here**.

RoC
Report on Compliance

- A RoC is a report that is created at the end of a PCI-DSS assessment by a QSA. This report shows that an organization is compliant and can be shared with the processors/banks to prove compliance. There are also executive summaries that are available to show compliance to other organizations you may support without having to share the entire report. Remember PCI-DSS is a Pass/Fail standard and one fail means the entire validation failed.

6 Financial Services

FDIC
Federal Deposit Insurance Corporation

- Organization that insures the deposits of American Banking Organizations in the United States of America.

NCUA
National Credit Union Administration

- Organization that insures the deposits of Credit Unions in the United States of America. NCUA is also a body who focuses on security audits to ensure their members meet the minimum requirements and continue to improve their security programs.

FFIEC
Federal Financial Institutions Examination Council

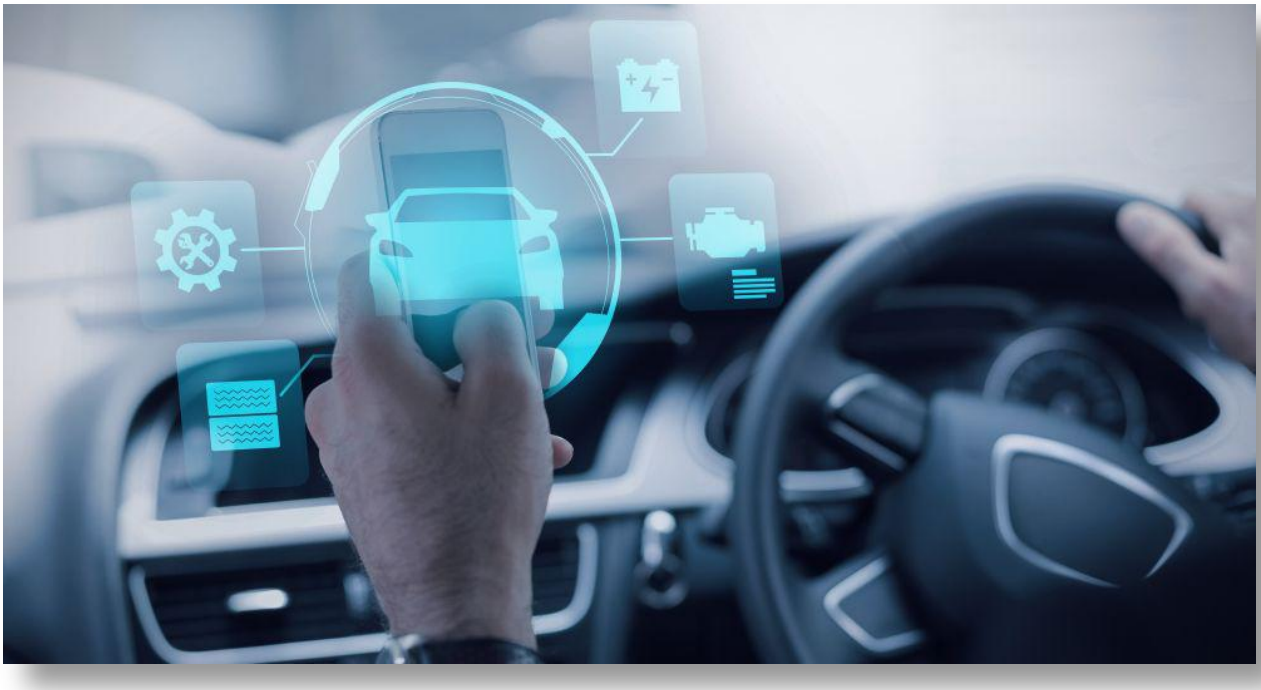
- This is a regulation body comprised of five major banking regulators. They focus on two areas. Housing & Real Estate and Cybersecurity. Banks are required to go through an annual FFIEC audit with a regulator once per year and as of June 30th, the FFIEC released their own Cyber Security Assessment Tool. If a bank fails or refuses to administer their cybersecurity, they can lose their FDIC Insurance.

Core Providers

- Many community Banks and Credit Unions are small organizations who require the assistance of 3rd party resources to accomplish their IT needs. The core providers administer services such as banking platforms, and ATM machines. It allows an organization to interconnect to offer services to their customers. These services can include but are not limited to online banking and ATM Machines.

SOX
Sarbanes-Oxley Act

- A law that was enacted on July 30th, 2002. This law's intent is to ensure the protection of financial reporting data.



7 Automotive Industry

OEM
Original Equipment Manufacturer

- These would be the Automakers. Some examples include:
    - Volkswagen
    - BMW
    - Diamler
    - General Motors
    - Ford Motor Company
    - Toyota
    - Kia
    - Tesla

TISAX
Trusted Information Security Exchange

- A security standard developed by a VDA user group specifically focused on cybersecurity. The intent of this standard is to protect data that is shared throughout the supply chain and other vendors. This type of data can include but is not limited to Prototype Data, Prototype Vehicles, and PII.
- Today this is excepted by the German OEMs and in some cases the OEMs will not allow a company to bid on a project unless they currently have the TISAX Label.

SGA
Simplified Group Assessment

- An assessment that is performed in TISAX when you have multiple sites, and have a mature Information Security Management System. This methodology of assessing for TISAX utilizes sampling, which allows for the ease of adding new sites to the certificate. In this methodology the headquarters site will have a more in depth assessment, where the specific sites will have a simpler assessment.

Participant Handbook

- A handbook that is offered **here**. This handbook walks organizations through the TISAX Assessment process from registration, to the audit, and all the way through actually receiving their labels. It provides many tips and useful hints on how an organization can set themselves up to complete a successful audit.

AL
Assessment Level

- When going through a TISAX Assessment it is required that you choose your assessment level. These assessment Levels are based upon what objectives have been chosen. To choose the objective and levels it is highly recommended that you work with your partner to ensure it meets their criteria.

AL 1
- This is a self-assessment of TISAX based upon the VDA ISA

AL 2
- This is an assessment completed by one of the accredited audit providers listed **here**. The purpose of an AL 2 is a validity check and is allowed to be completed offsite unless an organization's location is on the Activation list.

AL3
- This is an exhaustive assessment that must be completed by one of the audit providers that are listed **here**. If you touch any sort of prototype data you will be required to complete an AL 3. An AL 3 is required to be performed onsite.

Label

- The name of the certification obtained by successfully completing a TISAX Assessment

Objectives

- A list of predetermined data types that an organization or in this case an OEM is trying to protect. These objectives include areas such as Prototypes, Data Privacy, and PII.

Objectives

- A list of predetermined data types that an organization or in this case an OEM is trying to protect. These objectives include areas such as Prototypes, Data Privacy, and PII.

No.	Assessment objective	Abbreviation
1.	Information with high protection needs	Info high
2.	Information with very high protection needs	Info very high
3.	Data protection According to article 28 (“Processor”) of the European General Data Protection Regulation (GDPR)	Data
4.	Data protection with special categories of personal data According to article 28 (“Processor”) with special categories of personal data as specified in article 9 of the European General Data Protection Regulation (GDPR)	Special data
5.	Protection of prototype parts and components	Proto parts
6.	Protection of prototype vehicles	Proto vehicles
7.	Handling of test vehicles	Test vehicles
8.	Protection of prototypes during events and film or photo shootings	Events + Shootings

Source: TISAX Participant Handbook section 4.3.3.6

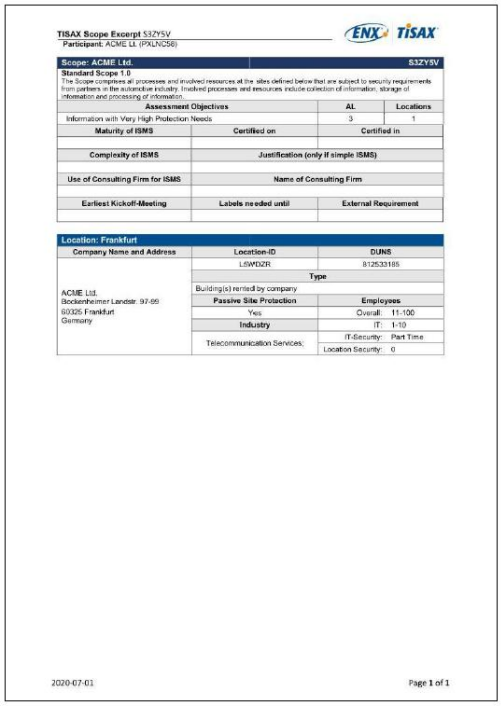
https://portal.enx.com/en-US/TISAX/downloads/

ENX
European Network Exchange

- The accreditation body that oversees TISAX

Scope Excerpt

- This is the required document that must be provided to Audit Providers for TISAX to be able to offer a quotation.


TISAX Scope Excerpt S3ZY5V
Participant: ACME Ltd. (PXLNDS8)

Scope: ACME Ltd. S3ZY5V
Standard Scope 1.0
The Scope comprises all processes and involved resources at the sites defined below that are subject to security requirements from partners in the automotive industry. Involved processes and resources include collection of information, storage of information and processing of information.

Assessment Objectives	AL	Locations
Information with Very High Protection Needs	3	1

Maturity of ISMS	Certified on	Certified in

Complexity of ISMS	Justification (only if simple ISMS)

Use of Consulting Firm for ISMS	Name of Consulting Firm

Earliest Kickoff-Meeting	Labels needed until	External Requirement

Location: Frankfurt

Company Name and Address	Location-ID	DUNS
ACME Ltd. Bockenheimer Landstr. 97-99 60325 Frankfurt Germany	LSWDZR	812533185
	Type	
	Building(s) rented by company	
	Passive Site Protection: Yes	Employees: Overall: 11-100
	Industry: Telecommunication Services	IT: 1-10 IT-Security: Part Time Location Security: 0

2020-07-01 Page 1 of 1

Source: TISAX Participant Handbook section 7.3

Activation List

- Although recently removed, this was a list of countries pre-determined by VDA that required an onsite TISAX assessment no matter what level assessment an organization was required to complete. If you are looking for this on the TISAX website, but don't find it, it was because it is no longer there.

VDA

- Verband Der Automobilindustrie (The German Association of the Automotive Industry)
- This is a German Interest Group for the Automobile Industry, the group is located in Berlin Germany. They represent car makers including BMW, Volkswagen, Diamler, and other foreign suppliers such as Opel.

SGA

- Simplified Group Assessment
  - The SGA is utilized for organizations looking to receive TISAX labels for an entire group. The benefits are simplified ways to add new locations to an overall label, corporate control, and the ability to utilize a sampling plan to reduce costs. To use the SGA you will need to have a mature Information Security Management System. The SGA has an annex document that can be used along with the participant handbook. The annex document is available along with the participant handbook located here.

ISA

- Internal Security Assessment
- For TISAX that VDA has put together. This assessment has the general assessment and subtabs that can be chosen based upon the objectives chosen.

ISO 21434

A standard that is currently under development for the Automotive World, with the intent of being released and required by automotive OEMs in 2023. This standard will take into account both cyber security and functional safety for the developed technology in on-road vehicles.

TSPIR

This standard very much competes with TISAX, however it specifically follows the US OEM requirements. In contrast to TISAX, a group from AIAG has wit members from GM, Ford, FCA, Honda and Toyota all contributing. The focus on this standard is NIST, however it can be cross referenced from a control standpoint to its counterpart ISO 27001.

AIAG

Automotive Industry Action Group

This is the US version of the VDA and is set up as a non-profit organization. Originally this group was set up to develop frameworks and recommendations for the improvement of quality.

8 Public Sector, Critical Infrastructure, and Defense

CMMC Cybersecurity Maturity Model Certification

A certification created to protect information shared with the DoD supply chain. The intent is to ensure that this sensitive information is being protected by manufacturers who historically overlook cybersecurity. To help the small manufacturers, DoD has provided reimbursable expenses which can be used by organizations to prepare themselves for a CMMC certification audit. These audits must be completed by 3rd party certification organizations who hold and maintain their C3PAO status.

CMMC Levels

These are assessment levels that an organization is looking to meet for certification.

	Processes	Practices
Level 5	Optimized	Advanced/Progressive
Level 4	Reviewed	Proactive
Level 3	Managed	Good Cyber Hygiene
Level 2	Documented	Intermediate Cyber Hygiene
Level 1	Performed	Basic Cyber Hygiene

Level 1

- This is the least mature model for CMMC, and the intent is to protect FCI. In this level, there are measures in place, however they may be limited and/or inconstant.

Level 2

- This level's intent is to progress from Level 1 and can be considered a maturity level stepping stone to Level 3.

Level 3

- The type of organization who looks to certify to Level 3 is an organization who requires access to CUI. This type of organization can show that it has good cybersecurity hygiene, and their controls will meet the requirements of NIST 800-171.

Level 4

- Organizations who meet Level 4 CMMC have shown they have a mature and adaptable cyber security program. They have specifically shown their ability to review their process for effectiveness and inform upper management of opportunities for improvement.

Level 5

- This is the highest level of maturity achievable in the CMMC program. These organizations have shown their ability to continually fine tune their programs, which leads to the ability to defend against APTs. The expectation of a Level 5 organization is that they have not only implemented the program, but that it has been implemented and is effective across their entire organization.

CFR
Code of Federal Regulations

- There are 50 titles in the CFR. These are the codification, rules and regulations that are published by the Federal Government

FCI
Federal Contract Information

- This information is generated by the DoD for contract purposes and is not intended for public release

CMMC AB
Cybersecurity Maturity Model Certification Accreditation Body

- The organization that oversees CMMC certification

APT
Advanced Persistent Threats

- This can be used as a stealth attack mostly for nation state purposes. Once on the network the hackers will remain undetected for an extended period of time.

C3PAO
CMMC Third Party-Assessor Organization

- The organization who is accredited to certify organizations to CMMC

CA
Certified Assessors

- These are the individuals that can perform audits under a C3PAO

LPP
Licensed Partner Publisher

- The organizations who create the content for CMMC training

LTP
Licensed Training Partner

- These are the companies who are able to provide training to organizations around CMMC

LI
Licensed Instructors

- These are the people who are able to deliver the training themselves and work for a LTP

RPO
Registered Provider Organization

- An organization who consults on CMMC, provides all services except the certification services. This designation notifies organizations that an RPA has accepted the terms of professional conduct

RP
Registered Practitioners

- These are the individuals who provide consulting on CMMC. They have passed the basic training on the CMMC standard

DoD
Department of Defense

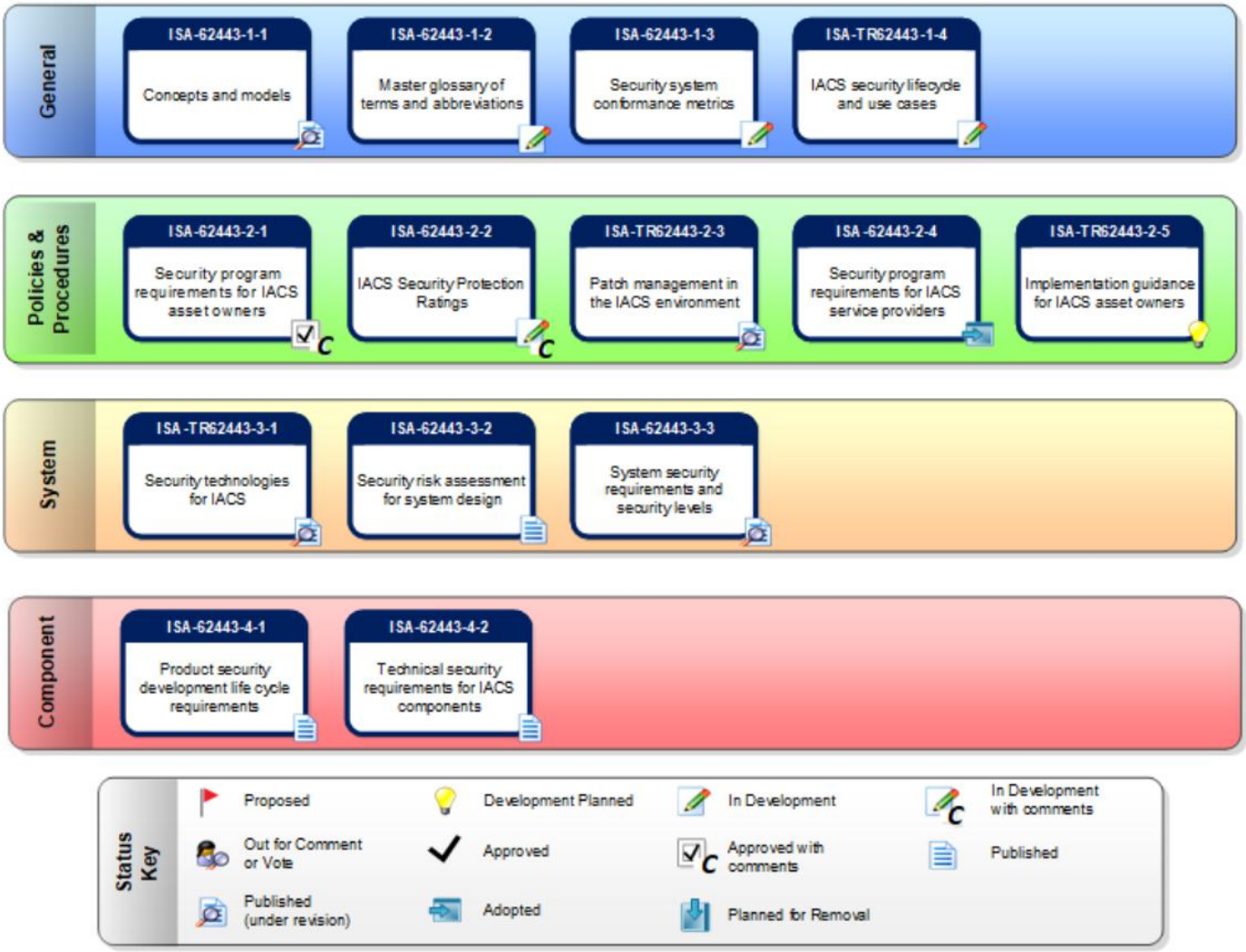
- The US department responsible for the oversite of all things national security and United States Armed Forces

CUI
Controlled Unclassified Information

- This is information that requires safeguarding

IEC 62443

- A series of standards and requirements for organizations who want to sell into the Critical Infrastructure Sector. Parts of this series focus specifically on product, where other parts focus on more of a traditional management system. The individual sub standards are listed below:
- Link to page **here**



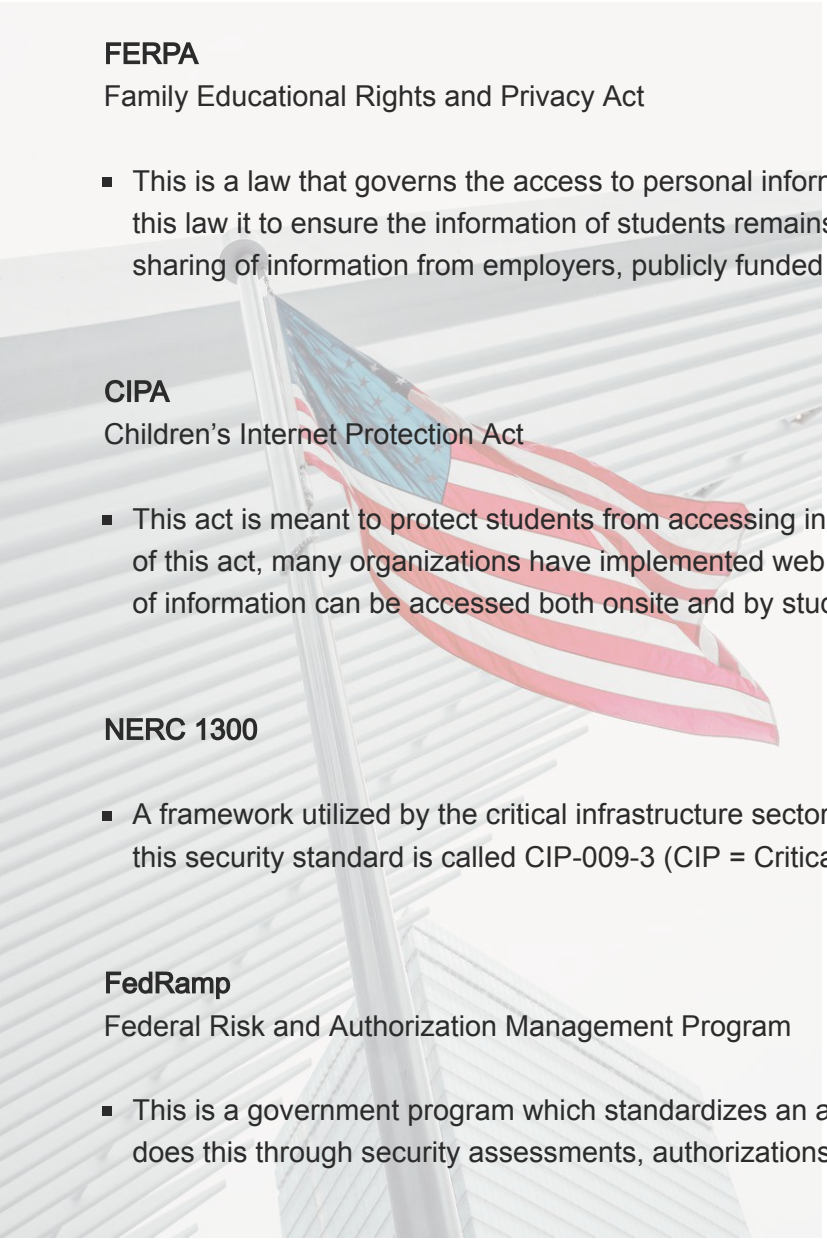
NIST 800-53

- Provides a wide range of security and privacy controls for an organization. This is not an accredited certification, however it is one of the most popular information security frameworks in the USA. The intent of this standard is to be used for all US Federal Information Security Systems that do no have national security information.

FERPA

Family Educational Rights and Privacy Act

- This is a law that governs the access to personal information held by educational organizations. The intent of this law it to ensure the information of students remains safe and secure, but has had a major impact on the sharing of information from employers, publicly funded educational institutions, and foreign governments.



CIPA

Children's Internet Protection Act

- This act is meant to protect students from accessing inappropriate and explicit content. Due to the ramifications of this act, many organizations have implemented web filters and other practices to regulate who and what types of information can be accessed both onsite and by students with district provided computers and devices.

NERC 1300

- A framework utilized by the critical infrastructure sector to protect SCADA assets. The most recent version of this security standard is called CIP-009-3 (CIP = Critical Infrastructure Protection).

FedRamp

Federal Risk and Authorization Management Program

- This is a government program which standardizes an approach to access of cloud products and services. It does this through security assessments, authorizations, and continuous monitoring of these systems

ITAR

International Traffic in Arms Regulations

- This regulation is meant to protect and control the export of defense and armed service technologies. The intent of this is to safeguard US National Security

9 Common Cybersecurity Attacks

Ransomware

- A type of malware that takes the information on a computer, network, or an entire organization and encrypts that information. Once encrypted the attacker asks for a ransom, usually in Bitcoin, and if the person/organization does not pay, they will lose it forever. Over the past year however, these attacks have started to take information from those who choose not to pay, and sell it on the darknet.

Man In the Middle

- This attack is where an attacker will sit between the connection and what the user believes is a secure connection to the website. Very similar to eavesdropping, an attacker is able to learn about specific sensitive information of a user or company.

Spoofing attack

- This is where an attacker cloaks or hides a device by providing fake data to a user or a network so it is believed that you are communicating with a trusted device or person. Commonly on a network spoofing attack, a hacker will make a network believe they are a printer, as printers' security authorizations tend to be weak.

Cross-Site Scripting

- An attack typically carried out on a web application, which focuses on inputting scripts into the web application that is used by others.

Phishing

Most commonly sent in email form, phishing is sent out to as many people as a malicious person can find in the attempt that someone will take the bait and either click on a link or download an attachment.

Spear Phishing

Similar to phishing, this is directed towards specific individuals and has targeted information about that person to gain higher chances of someone falling for their trap.

See *phishing* example below:

tuvsud.com Microsoft account unusual sign-in activity Edward.Chandler@tuvsud.com

MA Microsoft account team <agui@thenavigatocompany.com>
To Chandler, Edward

Retention Policy Junk Email (30 days) Expires 11/19/2020

This item will expire in 29 days. To keep this item longer apply a different Retention Policy.
If there are problems with how this message is displayed, click here to view it in a web browser.

"Attention! External Mail. Be careful with Links/Attachments!"

Microsoft Office 365

Hi Edward.Chandler

Our records indicated that you recently made a request to terminate your account. You will loose all your emails associated with your account

If you have no knowdledge about the request process,kindly cancel the request below and also receive pending emails.

You'll need to login with your valid password to rectify your account,after 3 failed attempts your account Edward.Chandler@tuvsud.com will be blocked.

Click here to retrieve pending messages to inbox.

Thanks,
The Microsoft account team

Denial of Service

- This type of attack is carried out by the amount of traffic that is hitting a webserver at one time. In 2012 and 2013, these attacks were very prevalent against financial institutions by the hacking group Anonymous.

Brute Force

- This is where an attacker will try passwords until they eventually guess the password correct. To make this quicker and easier, now hackers have the ability to run programs that will try millions of passwords per second making it a fairly fast task of gaining access to a system. This is the precise reason companies have minimum password requirements, as the more complex a password is, the harder it is to guess.

Insider Attack

- When someone within an organization becomes malicious in their intent. Typically referred to as rogue employees, the trusted access an individual has to a network can be extensive, especially with networks that are considered “flat”. A common misconception behind cyber attacks is that the majority of them come externally, where the truth is that it is actually more likely for an attack to come from inside the network.

Zero Day

- This is a software vulnerability that is unknown to the makers and/or maintainers of the program who have the ability to mitigate the risk. This gives attackers the ability exploit these vulnerabilities.

Drive-by Attack

- This is an unintentional download of software to a device that will leave that device vulnerable to future attacks.

Trojan Horse

- This is exactly as the Greek story described, except in computer terms… This is where malware is disguised as something that it is not and misleads users of its actual intent.

Directory Traversal

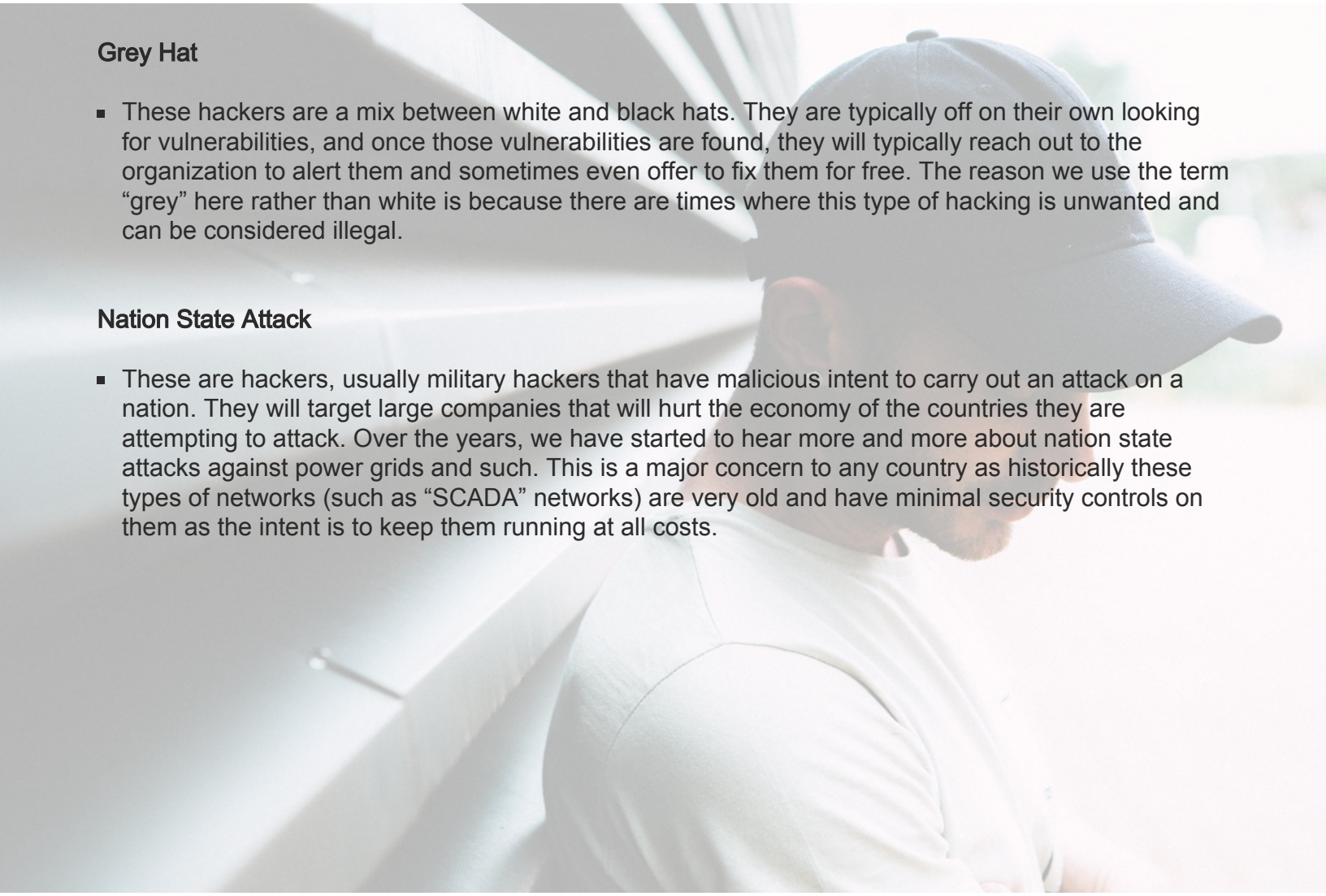
- This is an attack where someone is able to gain access to files and folders that would be restricted from them, by running commands that are outside of the webserver's root directory.

White Hat

- An ethical hacker who breaks code and programs to better their security.

Black Hat

- An unethical hacker, usually a criminal. This person is trying to break code or programs for malicious purposes such as but not limited to: financial, defacing, or nation state.

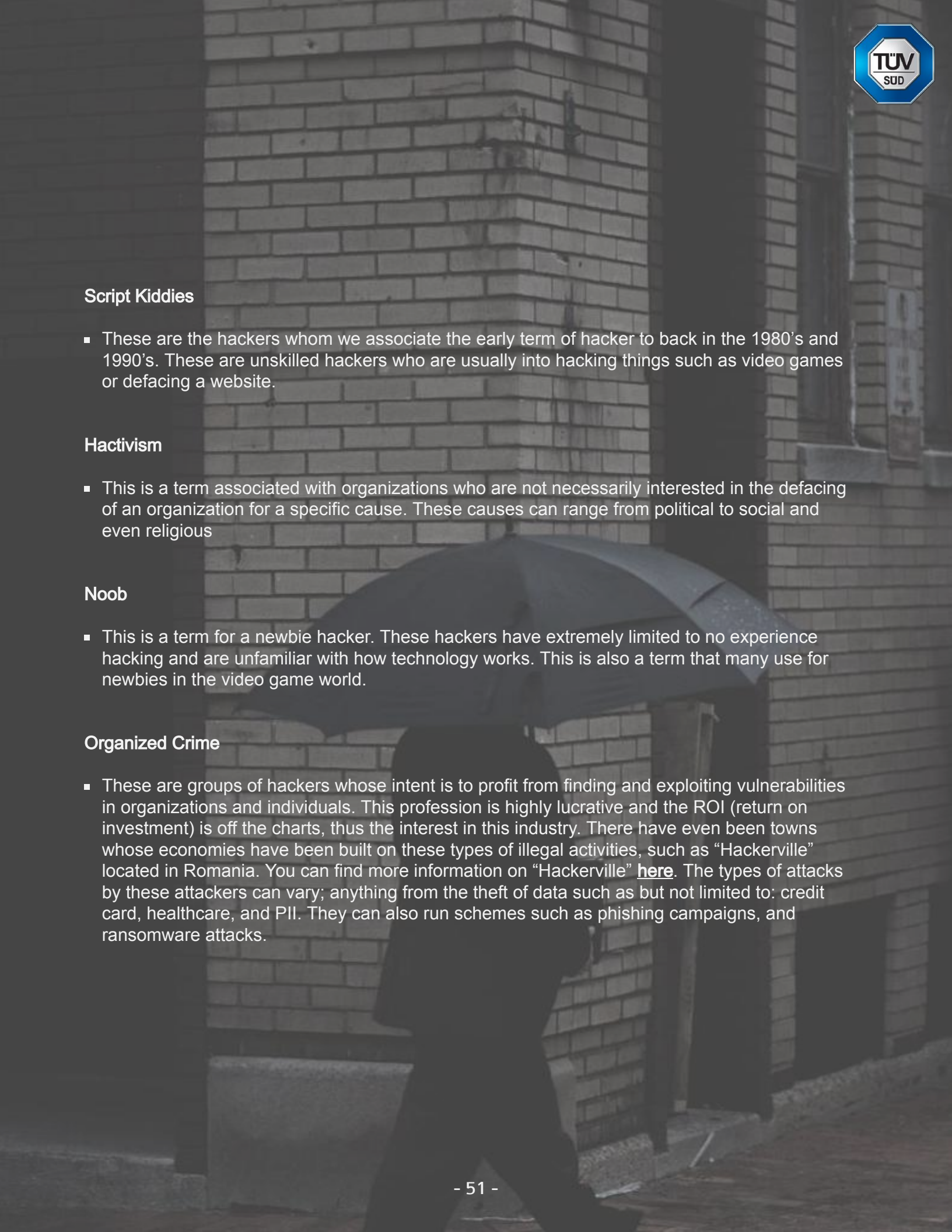


Grey Hat

- These hackers are a mix between white and black hats. They are typically off on their own looking for vulnerabilities, and once those vulnerabilities are found, they will typically reach out to the organization to alert them and sometimes even offer to fix them for free. The reason we use the term "grey" here rather than white is because there are times where this type of hacking is unwanted and can be considered illegal.

Nation State Attack

- These are hackers, usually military hackers that have malicious intent to carry out an attack on a nation. They will target large companies that will hurt the economy of the countries they are attempting to attack. Over the years, we have started to hear more and more about nation state attacks against power grids and such. This is a major concern to any country as historically these types of networks (such as "SCADA" networks) are very old and have minimal security controls on them as the intent is to keep them running at all costs.



Script Kiddies

- These are the hackers whom we associate the early term of hacker to back in the 1980's and 1990's. These are unskilled hackers who are usually into hacking things such as video games or defacing a website.

Hactivism

- This is a term associated with organizations who are not necessarily interested in the defacing of an organization for a specific cause. These causes can range from political to social and even religious

Noob

- This is a term for a newbie hacker. These hackers have extremely limited to no experience hacking and are unfamiliar with how technology works. This is also a term that many use for newbies in the video game world.

Organized Crime

- These are groups of hackers whose intent is to profit from finding and exploiting vulnerabilities in organizations and individuals. This profession is highly lucrative and the ROI (return on investment) is off the charts, thus the interest in this industry. There have even been towns whose economies have been built on these types of illegal activities, such as "Hackerville" located in Romania. You can find more information on "Hackerville" **here**. The types of attacks by these attackers can vary; anything from the theft of data such as but not limited to: credit card, healthcare, and PII. They can also run schemes such as phishing campaigns, and ransomware attacks.

Add Value. Inspire Trust.

TÜV SÜD is a global provider of auditing and certification services. Our in-depth knowledge of regulatory compliance around the world and our highly experienced auditors provide you with a fast, efficient service. We focus on helping you become more consistent, efficient and compliant – which means you bring products to market faster, avoid liabilities and boost profits.

TÜV SÜD America 10 Centennial Drive, Peabody, MA 01960
(800)-888-0123 info-us@tuvsud.com www.tuvsud.com/en-us