Issue 2 | April | 2024

Terminus Shield

GDPR COMPLIANCE IS WHAT YOU MUST BE AWARE OF

Our goal is to increase the level of awareness of the audience about the latest topics on information security, so with sending your feedback and comments, help us to do it better.

info@terminusys.com

From the Editor

Organizations collect and process a huge amount of personal data for their daily operations. Most of the time, individuals have little or no awareness about how much of their personal data resides in various organizations' databases. As an organization stores more and more personal data, its risk of data loss or a data breach goes up. To avoid these security risks, many groups are calling for regulations that:

- Set high standards of privacy and security in personal data processing and retention.
- Offer individuals more visibility and control over who has their personal data, how it's collected, how long it will be retained, and what it will be used for.

The General Data Protection Regulation (GDPR) is Europe's newest data protection law, designed to unify and improve the privacy of personal data across Europe. The GDPR intends to provide European Union (EU) residents with more visibility and control over the way their personal data is collected and processed.

There are 99 articles and 173 recitals in the GDPR that establish all obligations and requirements that organizations will have to comply with when the GDPR goes into full effect on May 25, 2018.

The GDPR applies to all businesses that:

- Operate in the EU.
- Process the personal data of EU residents (regardless of location).
- Provide goods or services to people in the EU (regardless of where processing takes place).

The GDPR focuses on securing and ensuring the privacy of EU citizens' personal and sensitive personal data.

So what's the difference between personal data and sensitive personal data?

The GDPR has defined six important principles on how personal data should be processed. It mandates that personal data shall be:

- Processed lawfully, fairly, and in a transparent manner (Lawful, fair, and transparent).
- Collected only for specified, explicit, and legitimate purposes. Data should not be further processed in a manner that conflicts with these initial purposes (Purpose limitation).
- Adequate, relevant, and limited to what is necessary (Data minimization).
- Accurate and, where necessary, kept up-to-date (Data accuracy).
- Processed in a way that data subjects can't be identified once their data has been used for its original purpose (Storage limitation).
- Processed in a manner that ensures security of personal data. This includes protection from accidental loss, destruction, or damage by implementing required technical and organizations measures (Data integrity and confidentiality).

Once the GDPR is enforced, organizations could face a few different penalties for non-compliance depending on the infraction. Possible consequences include:

- Suspending all data processing.
- Paying a fine of up to four percent of their annual worldwide turnover or 20 million euros—whichever is higher.
- Other sanctions including warnings, reprimands, and corrective orders.

The GDPR aims to regulate how organizations collect, store, process, and transfer personal data. The following five-step action plan provides a holistic approach to help you on your journey towards GDPR compliance.

Discover

Know where personal data lies.

The first step towards GDPR compliance is identifying where personal data resides. An inventory of your organization's personal data is a prerequisite for GDPR compliance. During the data discovery phase, you need to know:

- Where and in what form personal data is stored.
- What types of personal data are stored.
- Who has access to personal data, including when, where, and how personal data is used.

Manage

Govern how personal data is shared and used.

After data discovery, the next step is to establish accountability in the flow of personal data within your organization. Enforce policies, rules, and regulations to ensure data handling, sharing, and storage techniques are in compliance with the GDPR. Some important questions organizations should answer during this phase include:

- What's the lawful basis for holding this personal data?
- Is any personal data shared with third parties? If so, why?
- How is personal data processed?
- How long can personal data be stored?
- How do we track a data subject's personal data?

Secure

Protect data from loss, misuse, and breaches.

The GDPR mandates that data be stored, processed, and shared in a manner that ensures its security. Depending on the type, context, location, and volume of personal data that your organization stores, you may need to implement measures such as encryption, pseudonymization, and anonymization toreduce the risk of data exposure. During the securing phase, you need to ask yourself:

- What technical and organizational measures are in place to safeguard personal data?
- Can you detect and respond to system infiltrations or data breaches in real time?
- Are regular data protection impact assessments being carried out?
- What are your organization's provisions for handling the data breach notification process?
- Is there a data security incidence response plan in place?

Revise and repeat

Regularly check and adapt the compliance process.

GDPR compliance isn't a one-shot exercise; it's a continuous process of keeping up with a consistently evolving compliance environment, changing technologies, and data privacy requirements to demonstrate compliance at any point of time

For more information about GDPR and how to implement it in your organization just contact us info@terminusys.com

What is BlockChain? Part 2

Blockchain History

The first work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta. They wanted to implement a system where documents' timestamps could not be tampered with or backdated. In 1992, Bayer, Haber and Stornetta incorporated Merkle trees to the design, which improved its efficiency by allowing several documents to be collected into one block.

The first blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto in 2008. It was implemented the following year by Nakamoto as a core component of the cryptocurrency bitcoin, where it serves as the public ledger for all transactions on the network. Through the use of a blockchain, bitcoin became the first digital currency to solve the double-spending problem without requiring a trusted authority and has been the inspiration for many additional applications.

In August 2014, the bitcoin blockchain file size, containing records of all transactions that have occurred on the network, reached 20 GB. In January 2015, the size had grown to almost 30 GB, and from January 2016 to January 2017, the bitcoin blockchain grew from 50 GB to 100 GB in size. The words block and chain were used separately in Satoshi Nakamoto's original paper, but were eventually popularized as a single word, blockchain, by 2016. The term blockchain 2.0 refers to new applications of the distributed blockchain database, first emerging in 2014. The Economist described one implementation of this second-generation programmable blockchain as coming with "a programming language that allows users to write more sophisticated smart contracts, thus creating invoices that pay themselves when a shipment arrives or share certificates which automatically send their owners dividends if profits reach a certain level." Blockchain 2.0 technologies go beyond transactions and enable "exchange of value without powerful intermediaries acting as arbiters of money and information." They are expected to enable excluded people to enter the global economy, protect the privacy of participants, allow people to "monetize their own information," and provide the capability to ensure creators are compensated for their intellectual property. Second-generation blockchain technology makes it possible to store an individual's "persistent digital ID and persona" and provides an avenue to help solve the problem of social inequality by "potentially changing the way wealth is distributed". As of 2016, blockchain 2.0 implementations continue to require an off-chain oracle to access any "external data or events based on time or market conditions [that need] to interact with the blockchain."

In 2016, the central securities depository of the Russian Federation (NSD) announced a pilot project, based on the Nxt blockchain 2.0 platform that would explore the use of blockchain-based automated voting systems. IBM opened a blockchain innovation research center in Singapore in July 2016. A working group for the World Economic Forummet in November 2016 to discuss the development of governance models related to blockchain. According to Accenture, an application of the diffusion of innovations theory suggests that blockchains attained a 13.5% adoption rate within financial services in 2016, therefore reaching the early adopters phase. Industry trade groups joined to create the Global Blockchain Forum in 2016, an initiative of the Chamber of Digital Commerce. In May 2018, Gartner found that only 1% of CIOs indicated any kind of blockchain adoption within their organizations, and only 8% of CIOs were in the short-term ‘planning or [looking at] active experimentation with blockchain’.

Blockchain Fundamentals

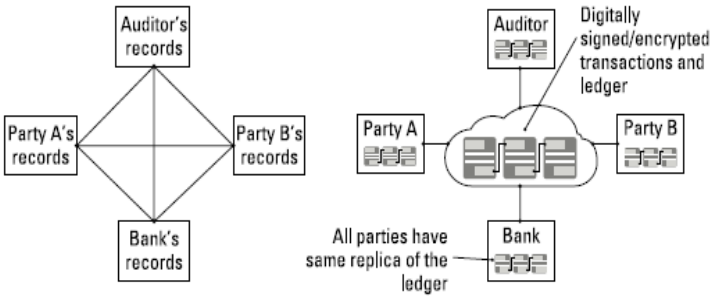
Blockchain is a shared, distributed ledger that facilitates the process of recording transactions and tracking assets in a business network. Each block typically contains a cryptographic hash of the previous block, a timestamp and transaction data. By design, a blockchain is inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

Blockchains are secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain. This makes blockchains potentially suitable for the recording of events, medical records, and other records management activities, such as identity management, transaction processing, documenting provenance, food traceability or voting. Blockchain was invented by Satoshi Nakamoto in 2008 for use in the cryptocurrency bitcoin, as its public transaction ledger. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server.

The bitcoin design has been the inspiration for other applications. An asset can be tangible like a house, a car, cash, land or intangible like intellectual property, such as patents, copyrights, or branding. Virtually anything of value can be tracked and traded on a Blockchain network, reducing risk and cutting costs for all involved. You can gain a deeper understanding of Blockchain by exploring the context in which it was developed — the need for an efficient, cost-effective, reliable, and secure system for conducting and recording financial transactions. Throughout history, instruments of trust, such as minted coins, paper money, letters of credit, and banking systems, have emerged to facilitate the exchange of value and protect buyers and sellers. Important innovations, including telephone lines, credit card systems, the Internet, and mobile technologies have improved the convenience, speed, and efficiency of transactions while shrinking and sometimes virtually eliminating the distance between buyers and sellers.

Still, many business transactions remain inefficient, expensive, and vulnerable, suffering from the following limitations:

- Cash is useful only in local transactions and in relatively small amounts.
- The time between transaction and settlement can be long.
- Duplication of effort and the need for third-party validation and/or the presence of intermediaries add to the inefficiencies.
- Fraud, cyberattacks, and even simple mistakes add to the cost and complexity of doing business, and they expose all participants in the network to risk if a central system, such as a bank, is compromised.
- Credit card organizations have essentially created walled gardens with a high price of entry. Merchants must pay the high costs of onboarding, which often involves considerable paperwork and a time-consuming vetting process.
- Half of the people in the world don't have access to a bank account and have had to develop parallel payment systems to conduct transactions.



Business networks before and after blockchain.

Transaction volumes worldwide are growing exponentially and will surely magnify the complexities, vulnerabilities, inefficiencies, and costs of current transaction systems. The growth of ecommerce, online banking, and in-app purchases, and the increasing mobility of people around the world have fueled the growth of transaction volumes. And transaction volumes will explode with the rise of Internet of Things (IoT) — autonomous objects, such as refrigerators that buy groceries when supplies are running low and cars that deliver themselves to your door, stopping for fuel along the way.

To address these challenges and others, the world needs payment networks that are fast and that provide a mechanism that establishes trust, requires no specialized equipment, has no chargebacks or monthly fees, and provides a collective bookkeeping solution for ensuring transparency and trust.

The birth of Blockchain

One solution that has been developed to address the complexities, vulnerabilities, inefficiencies, and costs of current transaction systems is bitcoin — a digital currency that was launched in 2009 by a mysterious person (or persons) known only by the pseudonym Satoshi Nakamoto.

Unlike traditional currencies, which are issued by central banks, bitcoin has no central monetary authority. No one controls it. Bitcoins aren't printed like dollars or euros; they're "mined" by people and increasingly by businesses, running computers all around the world, using software that solves mathematical puzzles.

Rather than rely on a central monetary authority to monitor, verify, and approve transactions and manage the money supply, bitcoin is enabled by a peer-to-peer computer network made up of its users' machines, akin to the networks that underpin BitTorrent and Skype.

Bitcoin has several advantages over other current transaction systems, including the following:

- Cost-effective: Bitcoin eliminates the need for intermediaries.
- Efficient: Transaction information is recorded once and is available to all parties through the distributed network.
- Safe and secure: The underlying ledger is tamper-evident. A transaction can't be changed; it can only be reversed with another transaction, in which case both transactions are visible.

Bitcoin is actually built on the foundation of Blockchain, which serves as bitcoin's shared ledger. Think of Blockchain as an operating system, such as Microsoft Windows or MacOS, and bitcoin as only one of the many applications that can be run on that operating system. Blockchain provides the means for recording bitcoin transactions — the shared ledger — but this shared ledger can be used to record any transaction and track the movement of any asset whether tangible, intangible, or digital. For example, Blockchain enables securities to be settled in minutes instead of days. It can also be used to help companies manage the flow of goods and related payments, or enable manufacturers to share production logs with original equipment manufacturers (OEMs) and regulators to reduce product recalls. In other words, Bitcoin and Blockchain are not the same. Blockchain provides the means to record and store bitcoin transactions, but Blockchain has many uses beyond bitcoin. Bitcoin is only the first use case for Blockchain.

With traditional methods for recording transactions and tracking assets, participants on a network keep their own ledgers and other records. This traditional method can be expensive, partially because it involves intermediaries that charge fees for their services. It's clearly inefficient due to delays in executing agreements and the duplication of effort required to maintain numerous ledgers. It's also vulnerable because if a central system (for example, a bank) is compromised, due to fraud, cyberattack, or a simple mistake, the entire business network is affected.

(continued in page 6)

Malware from A to Z Part 2

Malware delivery methods

Malware can be delivered in any number of ways, which are:

- Instant Messenger applications
- IRC
- Removable devices
- Attachment
- Legitimate "shrink-wrapped" software packaged by a disgruntled employee
- Browser and email software bugs
- NetBIOS
- Fake programs
- Untrusted sites and freeware software
- Downloading files, games, and screensavers from Internet sites

But in keeping in line with our "more birds, fewer stones" mantra, let's focus on the most common delivery methods first.
To that end, here are two basic scenarios you should be well prepared to face:

- Infection via spam emails with malicious attachments
- Infection via malicious RDP access (brute-forced or via stolen credentials)

Considering email represents direct access to the most vulnerable part of your network (your users), it's no surprise it's criminals' preferred channel for distributing malware. According to Verizon's 2018 Data Breach Investigations Report, an astounding 92.4% of malware was delivered via email. Compare that to 6.3% that was delivered via malicious or compromised websites.
In addition, Symantec's 2018 Internet Security Threat Report asserts that, of the malicious emails the company observed in 2017, 88% utilized email attachments while only 12% utilized malicious URLs. So attackers clearly don't mind playing favorites. When it comes to distributing malware, emails and, more specifically, email attachments are their obvious go-to.
But what types of attachments are they using? According to Symantec, the most popular file types are script files (.vbs and .js), followed by .exe's, .jar files, and Microsoft Word documents. Webpage files (.html, .htm), Windows script files (.wsf), PDFs, Excel files, and .rtf files also make the cut. Looking at that list, two things jump out. First, many of these file types are malicious scripts. Attackers are increasingly relying on scripts rather than traditional malicious binaries because they provide rich functionality and are often more difficult for traditional antivirus solutions to block. For that reason, while it may not always be practical, one thing to consider is restricting or disabling users' ability to run scripts altogether.
Even if you can't disable scripts at the endpoint level, however, filtering them out at the email level is definitely something worth considering. In fact, due to the risks script files pose, Google has added many to its list of file types blocked in Gmail. Unless your organization specifically requires otherwise, you would be well-suited following their lead and blocking all of the following:
.ADE, .ADP, .BAT, .CHM, .CMD, .COM, .CPL, .DLL, .DMG, .EXE, .HTA, .INS, .ISP, .JAR, .JS, .JSE, .LIB, .LNK, .MDE, .MSC, .MSI, .MSP, .MST, .NSH .PIF, .SCR, .SCT, .SHB, .SYS, .VB, .VBE, .VBS, .VXD, .WSC, .WSF, .WSH
Second, many of the attachments on the Symantec list are widely-used legitimate file types that often can't be categorically blocked. That's obviously a strategic decision on the part of attackers, who know their best chance of sneaking malicious code past gateway filters is by smuggling it inside legitimate file types. While you likely won't be able to filter out all of these file types at the email level (Office files, especially).
While malicious email attachments may be responsible for triggering the lion's share of malware infections, they're far from the only delivery option available to criminals. A growing number of criminals have turned their attention to targeting another vulnerable access point: Remote Desktop Protocol (RDP).
RDP was developed by Microsoft as a remote management tool particularly useful for offsite admins. It is commonly exposed in internal networks for use in administration and support, but when exposed to the wider Internet it can be a dangerous beacon for attackers. Identifying servers with vulnerable RDP connections (port 3389 is default) has been made incredibly easy thanks to scanning tools like Shodan and masscan. From there, it's simply a matter of applying brute-forcing tools like NLBrute to crack the RDP account credentials, and attackers are in.
Alternatively, if attackers are feeling especially lazy they can simply head over to the underground marketplace xDedic, where RDP access to a compromised server can cost as little as $6.
RDP has become a favorite infection vector for ransomware criminals, in particular, with the actors behind SamSam, CrySiS, LockCrypt, Shade, Apocalypse, and other variants all getting in on the act. Of these, SamSam has generated the most attention, infecting such high-profile targets as the City of Atlanta, electronic health records provider Allscripts, the Colorado Department of Transportation, and others.
The good news is there are relatively simple steps you can take to make RDP off limits to attackers:

- Restrict access behind firewalls and by using a RDP Gateway and/or VPNs
- Use strong passwords and two-factor authentication
- Limit users who can log in using RDP
- Implement an account lockout policy to help thwart brute force attacks

Taking these precautions is critical since attackers who gain access via RDP typically then have a strong foothold on the machine with local admin privileges. Once initial access has been established, attackers typically don't waste time scouting out the network and laying the groundwork for a large-scale infection.

Malware prevention

COMMON INFECTION VECTORS	PREVENTION
Email attachments	Block commonly abused file types (.vbs, .js, .exe, .jar, .html, .htm, .wsf, .bat, .lnk, .zip, .7z, etc.) User awareness training
Web (including URLs in emails)	Web filtering Ad blocking Patch management

(to be continued in next issue)

Modified Cyber Resiliency Model

Figure 3a graphically represents the Zobel et al. characterization of a resiliency profile for a slow-onset single-event cyberattack. In this case, the loss of quality of service occurs gradually over time, a virus gradually propagating across the system unnoticed. The start of the cyberattack in the timescale is represented as t0 start, the end of cyberattack is presented as t0 end, and the corresponding of loss of functionality is Q'(t). The time to recover the full functionality from t0 start is T. The triangular area with the base as T and the height as Q'(t) represent the loss of resiliency.

The smaller the area under the resiliency curve the system is more resilient. That is, the cyberattack did not impact the functional performance, or the system recovered quickly and/or a combination of both.

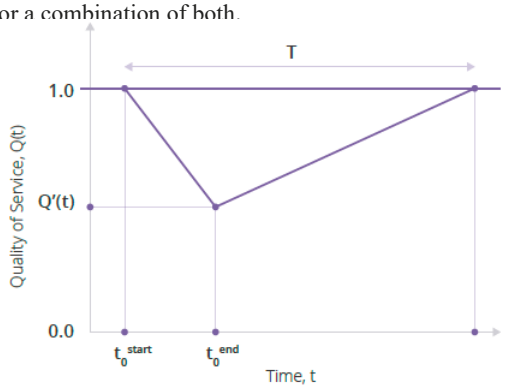


Figure 3a

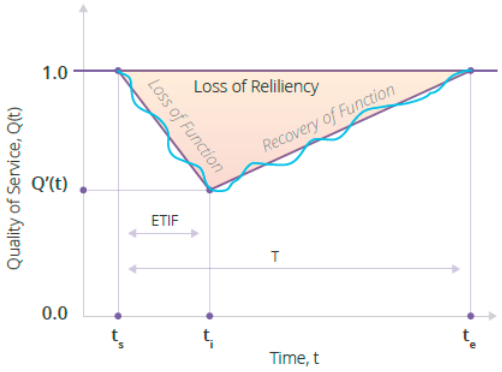


Figure 3b

Figure 3b represents the modified cyber resiliency model. In a typical cyberattack, the failure is identified by studying the anomaly/degradation of intended functions at the IDS layer. Therefore, the modified resiliency model starts with the time at which the failure was identified ti (in Zobel et al. model is t0 end, and the corresponding loss of function is Q'(t). Immediately after the identification of a failure, an investigation would start to identify the root causes of failure and to implement recovery actions to restore full functionality. The investigation would identify the time at which the cyberattack started, ts (in Zobel et al.'s model is t0 start). The line connecting ti to ts represent the loss of function. The duration between the start of the failure and the identification of the failure is defined as the Elapsed Time to Identify Failure (ETIF). The recovery actions would fix the failure, necessary to achieve full functionality. The time at which full functionality is achieved is represented as te. The line connecting ti and te represents the recovery function. Therefore, the modified resiliency model includes ETIF and the slopes of loss and recovery of functions, Figure 3b.

Cyberattacks occur when the information system vulnerabilities are exposed and exploited. For a given information system, these vulnerabilities are embedded into the architecture of the software and the hardware and characterize the attack surface As noted earlier, resilience of a system is characterized by its ability to achieve its intended functions despite disruptions. From that perspective, the bounding function on how a system is attacked and recovers is dependent on the attack surface. Thus, the functions representing resiliency, in this case ETIF, are bounded by the attack surface. These functions can be linear or non-linear; for illustrative purposes, the graphical information presented in this paper show linear relationships. However, discussions are certainly valid for both linear and non-linear functions.

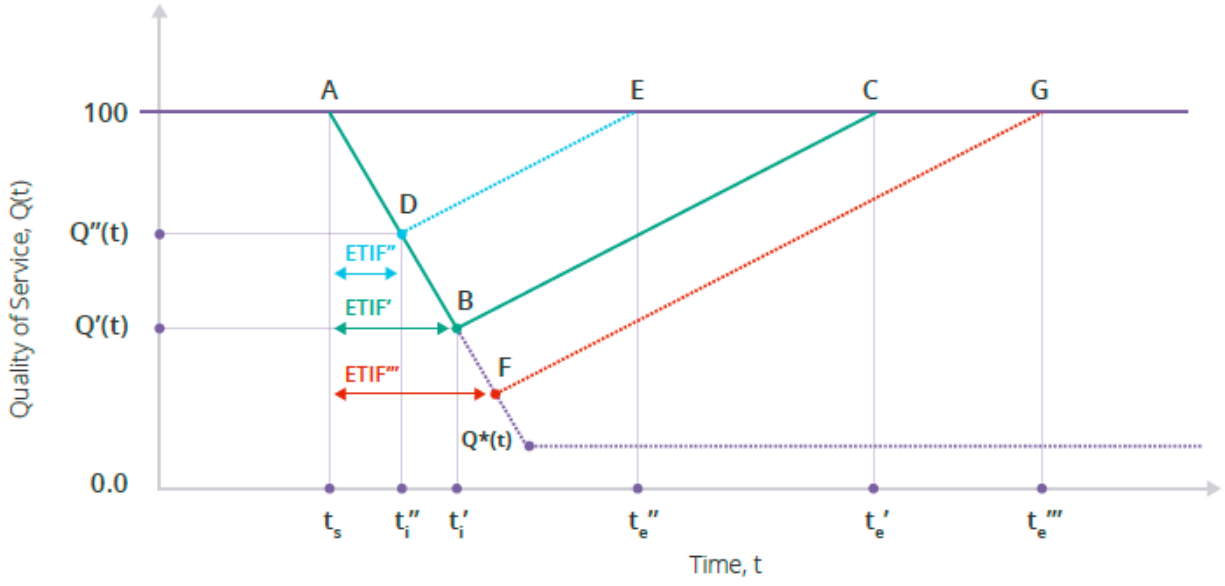


Figure 4

ETIF measures the loss of resiliency of an information system. If ETIF moves from ETIF' to ETIF'',
Figure 4, then the loss of resiliency area would reduce from triangle ΔABC to triangle ΔADE, the loss of quality of service, Q(t), would reduce from Q'(t) to Q''(t), and the recovery time (te) would reduce from te' to te''. Extending this argument, the loss of resiliency would reduce to zero when ETIF approaches zero. That is, the start of the cyberattack (t0) and the identification of the cyberattack (ti) occurred at the same time (i.e., the cyberattack was nullified at the IT/OT infrastructure.)
If ETIF moves from ETIF' to ETIF''', Figure 4, then the loss of resiliency area would increase from
ΔABC to triangle ΔAFG, the loss of quality of service, Q(t), would increase from Q'(t) to Q'''(t), and the recovery time (te) would increase from te' to te'''. However, if ETIF continue to increase, at some point the loss of resiliency reaches a level beyond which the system is not recoverable. This condition would be reached either when the quality of service, (Q(t), reached a point of no recovery, Q*(t), or when the cost of recovery is more than that to build a new information system, Figure 4. An example of this condition would be a security breach at a power generation company causing an electric generator to have a catastrophic failure resulting in a total loss of functionality. In this case recovery may not be possible.

(to be continued in next issue)

What is BlockChain? (Continue)

The Blockchain architecture gives participants the ability to share a ledger that is updated, through peer-to-peer replication, every time a transaction occurs. Peer to peer replication means that each participant (node) in the network acts as both a publisher and a subscriber. Each node can receive or send transactions to other nodes, and the data is synchronized across the network as it is transferred.
The Blockchain network is economical and efficient, because it eliminates duplication of effort and reduces the need for intermediaries. It's also less vulnerable because it uses consensus models to validate information. Transactions are secure, authenticated, and verifiable. The participants in both transaction systems are the same. What has changed is that the transaction record is now shared and available to all parties.
A Blockchain network has the following key characteristics:

- Consensus: For a transaction to be valid, all participants must agree on its validity.
- Provenance: Participants know where the asset came from and how its ownership has changed over time.
- Immutability: No participant can tamper with a transaction after it's been recorded to the ledger. If a transaction is in error, a new transaction must be used to reverse the error, and both transactions are then visible.
- Finality: A single, shared ledger provides one place to go to determine the ownership of an asset or the completion of a transaction.

Blockchain benefits for business

For business, Blockchain has the following specific benefits:

- Time savings: Transaction times for complex, multi-party interactions are slashed from days to minutes. Transaction settlement is faster, because it doesn't require verification by a central authority.
- Cost savings: A Blockchain network reduces expenses in several ways:
    - Less oversight is needed because the network is self-policed by network participants, all of whom are known on the network.
    - Intermediaries are reduced because participants can exchange items of value directly.
    - Duplication of effort is eliminated because all participants have access to the shared ledger.
- Tighter security: Blockchain's security features protect against tampering, fraud, and cybercrime. If a network is permissioned, it enables the creation of a members-only network with proof that members are who they say they are and that goods or assets traded are exactly as represented.

Not all Blockchains are built for business. Some are permissioned while others aren't. A permissioned network is critical for a Blockchain for business, especially within a regulated industry. It offers:

- Enhanced privacy: Through the use of IDs and permissions, users can specify which transaction details they want other participants to be permitted to view. Permissions can be expanded for special users, such as auditors, who may need access to more transaction detail.
- Improved auditability: Having a shared ledger that serves as a single source of truth improves the ability to monitor and audit transactions.
- Increased operational efficiency: Pure digitization of assets streamlines transfer of ownership, so transactions can be conducted at a speed more in line with the pace of doing business.

Building trust with Blockchain

Blockchain enhances trust across a business network. It's not that you can't trust those who you conduct business with; it's that you don't need to when operating on a Blockchain network. Blockchain is particularly valuable at increasing the level of trust among network participants. Because every transaction builds on every other transaction, any corruption is readily apparent, and everyone is made aware of it. This self-policing can mitigate the need to depend on the current level of legal or government safeguards and sanctions to monitor and control the flow of business transactions. The community of participants does that. Where third-party oversight is required, Blockchain reduces the burden on the regulatory system by making it easier for auditors and regulators to review relevant transaction details and verify compliance.

(to be continued in next issue)