eclypses + APEXAIQ™

WHITE PAPER

Next Generation of Best Practices in Data Security

New and emerging technologies will drive digital transformation across most industries, will your company be ready?

Document ID: ECLYPSES - 1532395320-273 2.0

Contents

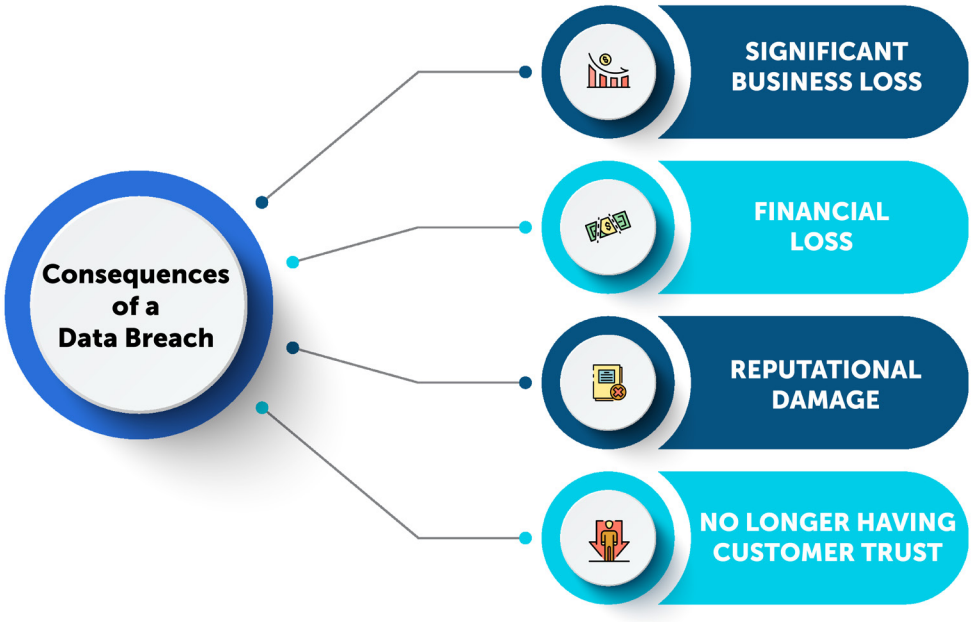
Introduction

Next generation (or NextGen) is a term often labeled to products and technologies to insinuate that the latest version of a product is new, different, and better than the previous version. When it comes to data security, there seems to always be the latest and greatest versions coming into play. How do companies determine what the next generation of best practices really are?

We have gathered data from industry experts to provide a list of future cyber threats to be ready for and what best practices you should consider for protecting your data today, and in the future.

Is Your Company Ready for the Future?

Protecting sensitive data is crucial for any business. With cybercrime up 600% due to the COVID-19 pandemic, it is important to have your data security systems ready for potential future threats. The consequences of a data breach can include significant business loss, reputational damage, financial loss, no longer having customer trust, etc. Cybercriminals are only becoming more sophisticated as they continue to discover new ways to steal your sensitive data.



Barely one in five organizations consider their organization prepared for a potential ransomware attack, according to Cybersecurity Dive. 60% of small companies go out of business within six months of falling victim to a data breach, according to Cybercrime Magazine. If most organizations are unprepared for today's cyberattacks, what will they do with future cyber threats?

Quantum Computing: The U.S. Cybersecurity and Infrastructure Security Agency (CISA) is warning government and critical infrastructure entities (both private and public) to act now to prepare against

emerging cyber threats with the onset of quantum computing. Quantum computing holds new security risks, as they have the potential to break encryption algorithms, and in the wrong hands, these powerful quantum computers could threaten U.S. national security.

The Security Risks of 5G: With 5G being an emerging platform, we need to be aware of the security risks that come along with it. "5G has great bandwidth and great configurability, but as people bring their technologies and services to market, the standards and the protocols are still emerging. Organizations like 3GPP or the internet engineering task force IETF or ITU are the bodies that continue to refine the standards, but we're still in the early days of those standards. They are built on mature predecessors, as the service providers attempt to adopt the standards and adhere to them. It is a moving target that presents a nascent set of new vulnerabilities, just like you do not buy the first model car when that car comes out. You don't want to buy the first model because the manufacturer probably has not worked out all the unique details where it hasn't been troubleshot yet, so we are in that early adopter phase of 5G," comments Scott Foote, CISO, Cybersecurity Executive, Managing Director, and Founder of Phenomenati.

Enhancements in Computing: Improvements in computing will enable today's cyber threats to grow and evolve. While current cyber strategies may protect you from present-day threats, these threats will mutate, and current securities will lag in defending against those mutations.

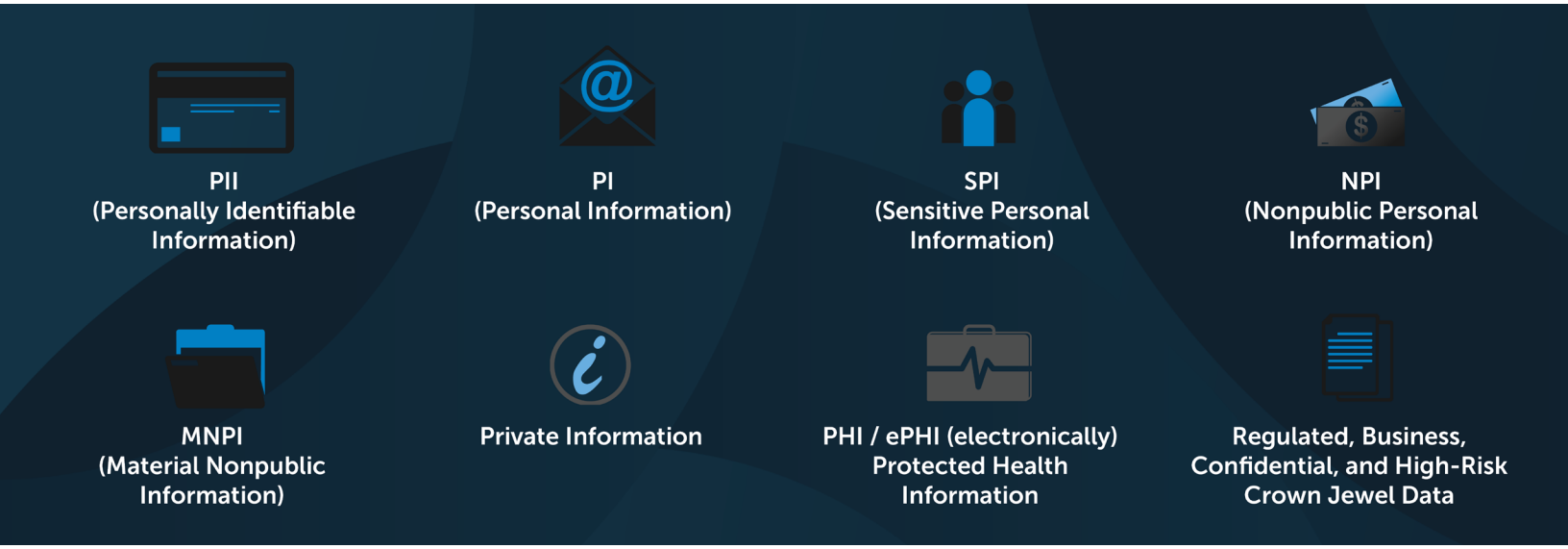
"This is where Eclypses MTE technology comes into play. MTE technology is designed to anticipate those mutations and still protect data no matter what," comments Aron Seader, Senior Director of Core Engineering at Eclypses. "Certain types of cyber-attacks will stick around, simply because they work, but we also need to be concerned about future threats. Consider adding technologies to your systems that focus on protecting your data for not only today – but tomorrow."

> ***"Certain types of cyber-attacks will stick around, simply because they work, but we also need to be concerned about future threats."***
>
> *- Aron Seader, Sr. Director of Core Engineering at Eclypses*

Best Practices in Protecting Your Data for Today and Against Future Threats

1. Identify your sensitive data

It is recommended to start by identifying what types of data you have in order to protect them successfully. Depending on your company and what industry you serve, sensitive data can vary from company to company. Once you classify what your sensitive data is, it needs to be protected at all times. According to BigID, types of sensitive data can include:



2. Train and educate your employees

“Humans are the weakest link, and it’s almost always due to lack of training or simple human error,” Scott Lowe, CEO, co-founder, and lead industry analyst at ActualTech, wrote in this report. Educating employees on possible cyber threats and best practices is the best way to reduce the risk posed by human error. Teaching them how to set up proper password security, what a phishing attempt looks like, and how to avoid viruses and hacking attempts are key to arming your employees with the skills they need to keep both company and personal data safe. Companies should implement training programs that employees are required to take in order to ensure that each employee is given all the information they need to understand the risks and rules they should follow. With proper training, employees will be able to stay safe from easily avoidable hacks, protecting the company as a whole.

3. Use multi-factor authentication (MFA)

Multi-factor authentication (MFA) or two-factor authentication (2FA) is an added layer of security used to ensure that it is you attempting to gain access to an account after a password has been entered. If a password has been compromised, having MFA in place can be the difference between a hacker gaining access to your information, or keeping it safe. By requiring employees to confirm their identity through both a password and another security measure, such as an authenticator app, MFA massively reduces the chances of a hacker successfully stealing account information and causing financial or reputational harm to your company. It is best practice to always require your employees to activate MFA on all their business accounts and even their personal accounts.

4. Use anti-virus and anti-malware

Implementation of anti-virus and anti-malware software onto all devices and networks is an important part of any company's security posture. Enterprise level anti-virus/malware solutions act as both a protection and alert system if a device or network is compromised by malicious code. Without these practices in place, a company's data is left open and vulnerable to attacks like spyware and ransomware.

Alongside anti-virus and anti-malware software, the company and employees must comply with best practices to ensure that the software is able to successfully protect the network and devices. This means not downloading unauthorized software from external networks and implementing receiver-side verification in mail servers to prevent as many potentially dangerous spam emails as possible from reaching employees.

5. Strong password policies

Maintaining strong password security is the first step in ensuring that your information stays protected from hackers. While this may seem simple on the surface, many people fall into bad password practices which allow their accounts to be easily accessed and stolen, costing companies millions. Here are a few key actions to encourage employees to have strong company password security:

Do not share passwords with anyone: The first rule that must be established is to never share a password with other people or store it in a place where it can be found and stolen. On desks, under keyboards, in notebooks, nowhere is completely secure against theft. Login credentials protect valuable information and no one, including the IT department, should be asked to have those credentials. Only the employee they belong to should have the information.

Lengthy and complex passwords are best: While it is important to create passwords that will be easy to remember, it is important that they are not easily guessed by others. Personal information, pets' names, family members' birthday, or any other information that is public-facing and could be found on social media are passwords that are too easily guessed. Encourage employees to use sentences or phrases that are at least 16 characters long and include numbers, symbols, and upper- and lower-case letters. These are best since they are much more complex and difficult to predict for hackers.

Use a different password for every account: Many people fall into the trap of using the same password for every account. Though it makes it easy for them to remember, it means that if one account is compromised, all of them are. It is important to encourage employees to use different passwords for all their accounts to prevent this vulnerability from becoming a problem.

Use multi-factor authentication (MFA): Implementing MFA provides an additional layer of security to an account that can help prevent hackers that steal a password from gaining full entry. Companies should require their employees to have MFA activated on all their business accounts and encourage them to do the same for their personal accounts.

6. Move away from session-based zero-knowledge security strategies

Current best practices are session-based methodologies that require handshaking and the exchange of credentials every time communication needs to take place. These exchanges of sensitive information at the beginning of each session are a huge target for many of the cyber-attacks we see today. By switching to NextGen security technology, such as MTE, the secure relationship between endpoints can persist between sessions and incorporate knowledge about a user or endpoint. This eliminates the need for handshaking and exchanging credentials, reducing the chance of session compromise and data exposure.

7. Back up your data

Copying or archiving your valuable information is considered a best practice. This back up is used to restore original information in the event of a data loss. It is important to make sure the backup is secure, and the access is limited.

8. Know your cyber insurance policy

Cyber insurance generally covers your business' liability for specific cyber events such as ransomware or a data breach. It is important to fully understand what your policy protects against. As some insurance companies, like Lloyd's of London, recently issued a statement that they will require its insurer groups globally to exclude catastrophic state-backed hacks from stand-alone cyber insurance policies. By not covering certain cyber-attacks, business will not be able to fight back.

9. Use endpoint security solutions that replace data at the application level

Unlike most solutions that stop at monitoring, Eclypses MTE technology takes a proactive approach to secure data at the application level. MTE technology utilizes Eclypses Cryptographic Library (ECL) to replace your data at the application layer, securing it before the operating system through any network until delivery to the receiving application.

With zero-day hacking attacks rapidly increasing, traditional security is unable to protect your organization's valuable data against these constant vulnerabilities. That is why MTE technology is different – this technology replaces your data with instantly obsolete random streams of values and restores it on the other side.

By securing at the application level, MTE technology:

- Verifies each endpoint connection
- Requires no change to the user experience
- Minimal impact on system resources
- Secures data inside the application
- Allows you to stop trusting the operating system and communication protocol

The bad actor would only see the MTE generated, instantly obsolete, random stream of values, which has no correlation to source data – don't just encrypt your data, replace your data.

10. Mitigate risk within your IT environment

As technology continues to evolve and become smarter and AI and IoT applications are being used more widespread, companies will need to truly understand their internal IT environments. But how can companies mitigate risk within their IT environment? With the use of IT Asset Management Systems such as Apexa iQ, you can see your entire IT estate within minutes. Without a platform like Apexa, CTO's and their team spend countless hours compiling data entries, manually at that, to present their entire IT estate. This can cause many complications because the data is manually entered, leaving room for error, the data can change overnight, especially those that reach end-of-life. And lastly, it takes up time and money for a company and their IT team.

The Apexa platform discovers your entire IT estate in minutes — on-premises, co-located and Cloud. With Apexa iQ, you can see every IT asset within your IT environment and get real time reporting on your IT environment. When you can see your entire environment, you can increase productivity, stay compliant and secure, and plan for future IT costs such as hardware refreshes and know exactly when that spend is needed. To date, Apexa iQ has helped companies save over $140M in technical debt and maintenance fees.

Apexa iQ best practices: understanding what devices are nearing or have reached EOL, obsolete, non-compliant, continuous patch management, expired warranties, real time accurate reporting, understanding your entire IT environment – know what you have, understanding your IT budget. With the integration of Eclypses MTE technology, the Apexa iQ platform's security will be stronger than ever, allowing Apexa iQ customers full endpoint to endpoint security.

"As someone who has come from the other side doing manual reports and spending so much time and effort gathering all devices and assets for the large bank I was working at, an IT asset management solution was the answer. This is why I built this platform – to help those doing manual reports mitigate complexity for their internal IT and stay secure," states Lokesh Aggarwal, Apexa iQ CEO.

Conclusion

Due to the exponential growth of data and the increase in cyber-attacks, you must look towards the future and create a robust data security strategy for your company. By implementing a strong data security solution and adhering to best practices, you will protect your information, build up your

reputation, be compliant with data security requirements, and reduce litigation expenses.

The next generation of digital transformation will help companies produce faster, smarter, and be able to handle complex situations easily. Will your company be ready? For more information, please contact Eclypses at **contact@eclypses.com** or Apexa iQ at **contact@apexaiq.com**.

Sources

Back to Basics: What's multi-factor authentication - and why should I care? (2022, May 16). NIST. Retrieved September 14, 2022, from https://www.nist.gov/blogs/cybersecurity-insights/back-basics-whats-multi-factor-authentication-and-why-should-i-care

Freeze, D. (2019, October 16). 60 Percent of Small Companies Close Within 6 Months of Being Hacked. Cybercrime Magazine. Retrieved September 14, 2022, from https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

Kapko, M. (2022, September 6). Most organizations remain unprepared for ransomware attacks. Cybersecurity Dive. Retrieved September 14, 2022, from https://www.cybersecuritydive.com/news/ransomware-preparedness-lacking/631174/

Nguyen, T. (2019, July 3). Antivirus Policy and Procedure Best Practices. Information Security Program. Retrieved September 14, 2022, from https://informationsecurityprogram.com/antivirus-policy-and-procedure-best-practices/

Password Best Practices. (n.d.). UC Santa Barbara Information Technology. Retrieved September 14, 2022, from https://www.it.ucsb.edu/secure-compute-research-environment-user-guide/password-best-practices

Preparing Critical Infrastructure for Post-Quantum Cryptography. (2022, August). cisa.gov. Retrieved September 14, 2022, from https://www.cisa.gov/sites/default/files/publications/cisa_insight_post_quantum_cryptography_508.pdf

PurpleSec. (2022, July 18). 2022 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends. Retrieved September 14, 2022, from https://purplesec.us/resources/cyber-security-statistics/#Cybercrime

Steele, K. (2022, May 4). A Guide to Types of Sensitive Information. BigID. Retrieved September 14, 2022, from https://bigid.com/blog/sensitive-information-guide/

ABOUT ECLYPSES

Eclypses has a disrupting cyber technology, offering organizations with an advanced data security solution not seen in today's environments, called MTE®.

Founded in 2017, Eclypses originated as a subsidiary of Secure Cloud Systems, Inc. with the primary focus of developing the MTE cyber technology to be the most innovative and disruptive data security solution for all mobile application technologies, websites, and IoT devices. The development of this technology led to the MTE toolkit, as we know it today.

Eclypses' patented MTE technology was developed through their technical team in Colorado Springs, CO, where they continue to innovate and expand on this cutting-edge security technology. The MTE technology generates a random string of values that is used to replace any form of structured or unstructured data. This replacement string of values is referred to as MTE, which provides innovative security against man-in-the-middle cyber-attacks.

This technology allows for a higher level of security to protect against man-in-the-middle cyber-attacks in products and applications that may have limited resources, such as battery life, processor, or throughput.

CONTACT

contact@eclypses.com
www.eclypses.com
(719) 323-6680

ABOUT APEXA iQ

ApexaiQ is a SaaS platform that gives you visibility into the hygiene of your entire IT environment on a single dashboard accompanied with a risk rating score and a path to remediate to improve that score. Status of Obsolescence, Maintenance, Compliance, Vulnerabilities, Rogue Devices and Crown Jewel Application Dependencies all in one spot.

No other solution identifies the status of so many elements effecting risk as ApexaiQ does. As a result, there is no better solution to help assess your environment and understand how to prioritize tasks to reduce risk. ApexaiQ's strong query engine enables powerful report such as KPI, SLA and Audit.

CONTACT

contact@apexaiq.com
www.apexaiq.com
(508) 685-2032