Eagle
CONSULTING PARTNERS

CYBERSECURITY FOR SUPERINTENDENTS

Why Investing Matters Now More Than Ever

A Roadmap to Protect Your Mission

CYBER RISKS ARE NOT ISOLATED TO THE IT DEPARTMENT

For Ohio County DD Boards, cyber risks are no longer isolated to the IT Department. Information security incidents represent critical risks to the agency's operations, disrupt services to the community, and can total hundreds of thousands or millions of dollars in financial impacts. DD Boards of all sizes cannot afford to downplay these risks.

To superintendents at small and medium county DD Boards, the challenges can seem insurmountable without the heftier budgets and sizeable IT Departments of Ohio's larger counties. Fortunately, agencies in smaller counties are just as capable of developing robust and secure information systems that provide many benefits to the Board.

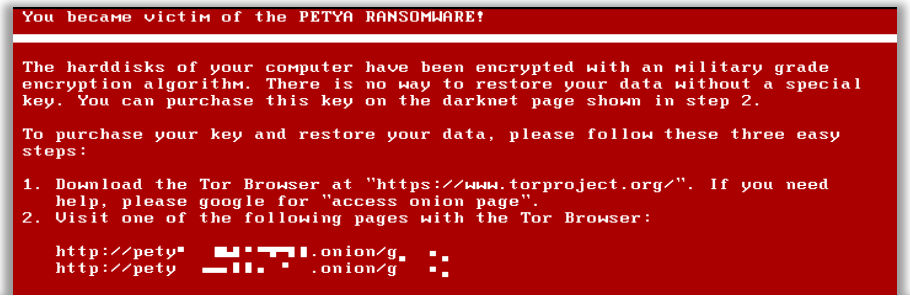
At Eagle Consulting Partners, we have 17 years of experience providing HIPAA compliance and information security risk management consulting to over 70 of Ohio's county Boards. We offer this white paper as a roadmap for small and medium DD Board leaders to follow.

This roadmap has four major themes:

1. Cyber threats to local government agencies like DD Boards have never been higher.
2. Boards must invest in secure information systems to avoid potentially crippling impacts and to improve operations and service delivery.
3. Information security can seem overwhelming, but Boards can achieve major benefits by just doing the basics well.
4. Board leaders don't have to go it alone. Instead, they should partner with experts and follow the examples of others.

In the following pages, we start by summarizing major information security risks and considerations for DD Boards. Then, we profile the Warren County Board of Developmental Disabilities, studying how this medium-sized county agency north of Cincinnati transformed their information systems from behind-the-times and insecure to modern, efficient, and secure. Finally, we summarize key lessons, pulled from the Warren County case study and Eagle's years of experience with county DD Boards, that superintendents and other leaders from small-to-medium-sized DD Boards can implement.

Cyber Threats to DD Boards Have Never Been Higher



What If All Board Computers Displayed This Ransomware Demand?

During any security risk assessment, we analyze three worst-case scenarios for a DD Board's information systems:

1. A major data breach that exposes all of the Protected Health Information (PHI) in the Board's IT systems.
2. Complete loss of all of the Board's data, including inability to restore or loss of backups.
3. Major operational disruption due to downtime or unavailability of critical IT systems.

Each of these scenarios typically has a very low likelihood of occurring, but the operational, reputational, and financial impacts of such an event would be significant. Responding to a major data breach could easily cost over $100,000 for all but the smallest of county agencies, with potential HIPAA fines of twice that amount. Complete loss of a Board's data, for instance due to an unrecoverable ransomware attack or other incident, would have financial impacts in the hundreds of thousands of dollars for smaller Boards such as Clinton, Holmes, or Preble Counties. For upper-medium-sized counties, on the order of a Warren, Lorain, or Mahoning County, the impacts could easily rise into the millions of dollars.

At the same time, superintendents need to consider the costs of IT and information security investments, the value of those investments, tradeoffs between security and usability, and the various regulatory compliance requirements.

It can be tempting for DD Board leaders to assume that their agency is already doing as much as they can. Or that, "it won't happen to us." Or even, "we can't do anything to stop it, so why try."

Unfortunately, the cyber risk to local government agencies like DD Boards has never been higher. Leaders cannot afford to bury their heads in the sand. According to a recent report:

> *"**In the first nine months of 2019, at least 621 government entities, healthcare service providers and school districts, colleges and universities were affected by ransomware.** The attacks have caused massive disruption: municipal and emergency services have been interrupted, medical practices have permanently closed, ER patients have been diverted, property transactions halted, the collection of property taxes and water bills delayed, medical procedures canceled, schools closed and data lost."*[i]

The list of victims includes over 68 state, county, and municipal entities. Cyber-criminal groups are specifically targeting local government agencies with ransomware and other malicious attacks because, quite frankly, most agencies are juicy targets. Agencies like DD boards, school districts, police departments, and public services are easy to infect with ransomware. They don't have the sophisticated IT systems, intrusion detection, or disaster recovery capabilities of bigger businesses. Employees are often susceptible to phishing or social engineering attacks. And the agencies have enough money in their budgets and insurance policies to pay sizeable ransom amounts, making the effort profitable for the bad guys.

The good news is that, with reasonable investments in the right areas of technology and security, DD Boards don't have to be victims.

Boards Must Invest in Secure Systems to Avoid Risk and Improve Operations

Warren County Board of Developmental Disabilities

The Example of Warren County Board of Developmental Disabilities

Eagle recently completed a computer security risk assessment for the Warren County Board of Developmental Disabilities, and we were impressed by what we found. Warren County is located between Cincinnati and Dayton. The DD Board serves over 1,800 individuals with developmental disabilities and employs 127 staff.[ii]

Of the many county DD boards and similar agencies where we have conducted risk assessments, Warren County DD Board has developed one of the more mature information security programs that we have seen. Under the leadership of Superintendent Megan Manuel and IT Manager Logan Stringer, the agency spent the last six years transforming their IT systems from outdated, slow, and vulnerable to modern, efficient, and secure.

Warren County Board's process of transformation provides an example that other DD Boards can follow. Manuel graciously let us profile her agency for this case study.

The Need for a Change

The process of what Manuel and Stringer refer to as their "five-year journey" started around 2012. At that time, the Board's IT systems were managed by the county IT department. County support services weren't always reliable. Additionally, the Board's computers and servers were aging, employees were tied to their desks for access to key applications like Gatekeeper, and maintenance activities such as patch management were inconsistent. Manuel candidly acknowledged that it was the operational impacts on her staff that really drove her to push for a change. Regarding any deficiencies in

Warren County DD Board Superintendent Megan Manuel

security and compliance, she said, "You don't know what you don't know, so you assume you are good."

Initially, Manuel and Stringer considered creating an in-house IT department. But the necessary skills and costs to build such a team became overwhelming. "We didn't know who to hire, even if we did try to do it internally," noted Stringer. They realized they needed to bring in outside expertise to handle the transition. A robust IT managed services company, they determined, would provide a wider range of skills and capabilities than Manuel and Stringer could ever build on their own, and at an equivalent or lower total operational cost than trying to hire a team and manage infrastructure internally. They also sought an IT company with the expertise with IT security and regulatory compliance necessary for the DD Board environment. After soliciting multiple proposals, Manuel and Stringer identified that GO Concepts, an IT services firm also based in Warren County, met their requirements.

Eagle has encountered GO Concepts on multiple DD Board engagements, and in 2018 we conducted a vendor evaluation of them on behalf of some of our DD Board clients. We found them to have good IT security controls and HIPAA compliance, appropriate to their size and business.[iii] These include:

- Well-trained staff familiar with IT security best practices and HIPAA requirements
- Reasonable diligence with HIPAA compliance
- Redundancy (internet connections, servers, backup power) for enhanced reliability
- Appropriate network design, including system and client isolation
- Data center physical security
- Attention to security operations, including use of industry leading tools for enterprise password management, remote monitoring, etc.
- Appropriate implementation of encryption, both in transit and at rest
- Evidence of a well-thought-out Disaster Recovery plan, including company-managed DR site
- Appropriate insurance coverage

Any IT managed services vendor working with DD Boards should have substantively similar qualifications.

"Five-Year Journey" Results

The partnership quickly flourished because Manuel and Stringer could articulate the Board's operational needs and GO Concepts could use their expertise and security perspective to recommend the right technical solutions. GO Concepts president John Gambill, Jr., described their approach as "trying to get people out of the IT business so they can focus their time on their core purpose."

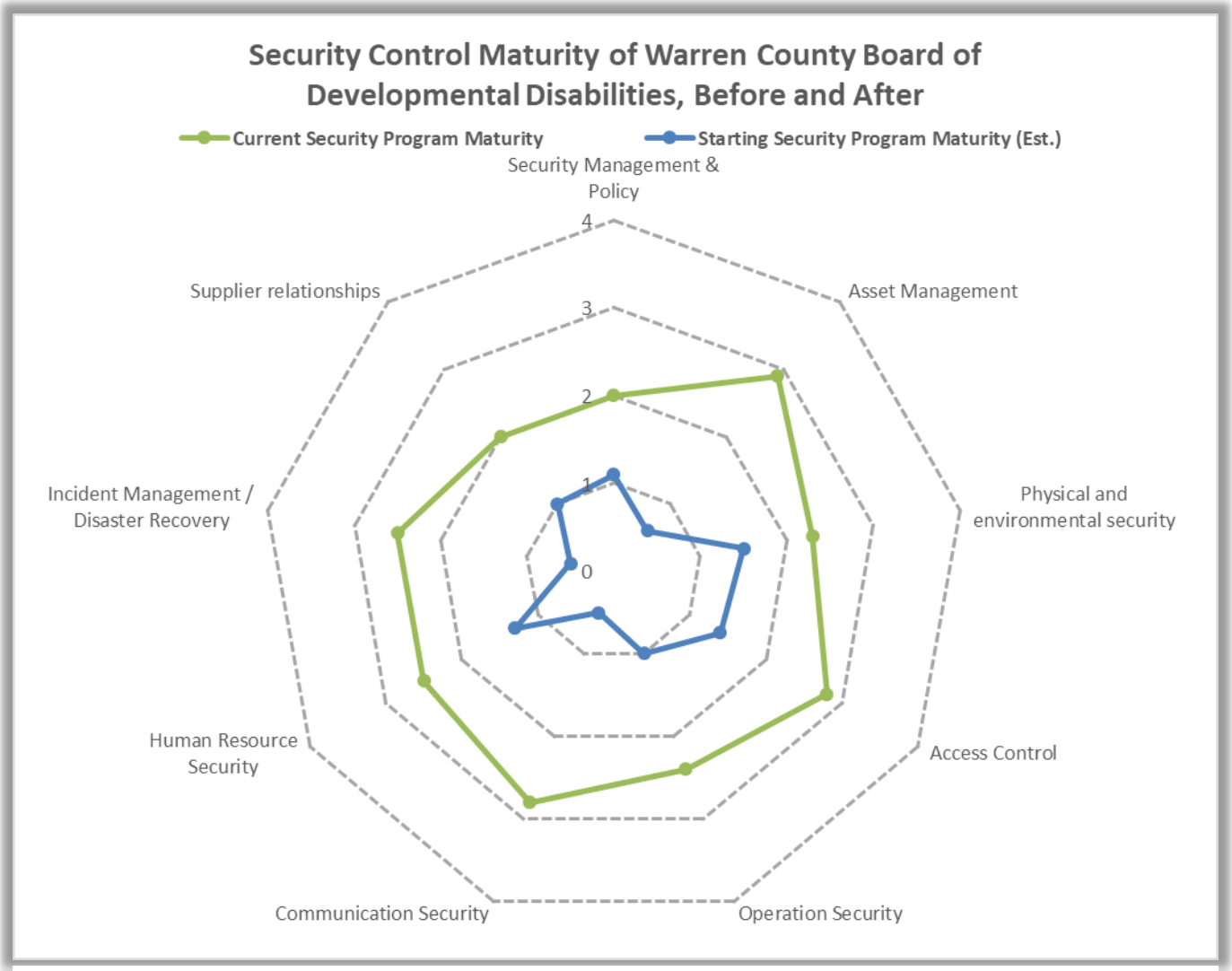
In order to replace their aging hardware, the Board migrated to GO Concepts' private cloud and centrally-managed remote desktop infrastructure, all running modern operating systems. This move greatly reduced the Board's risks from outdated, vulnerable systems, in addition to the day-to-day performance benefits. GO Concepts implemented secure configurations on all of these systems through their centralized management. They also keep the Board's systems up-to-date with patches and security updates, protecting against known vulnerabilities, and they monitor the network and firewall for potential concerns.

Through this partnership, the Board implemented secure remote access to the network, allowing Service Coordinators and other mobile staff to access Board systems from the field while keeping the data protected. The Board also took advantage of GO Concepts' robust system backup capabilities and Disaster Recovery data center. Effective backup and Disaster Recovery are critical for overcoming serious security incidents such as a major ransomware attack.

Further improvements provide layers of protection against the most common means of infection: compromising a user through a phishing email or malicious download. First, email filtering prevents most phishing attempts from reaching a user's inbox. Web filtering protects against links to malicious websites that might try to install malware. Second, an ongoing security awareness program for all staff, including simulated phishing assessments, educates employees to be security defenders. Third, managed antivirus/antimalware protects the computers themselves.

Most recently, Manuel and Stringer brought in Eagle Consulting Partners for a security risk assessment. We found that their work over the last few years, starting with hiring a well-qualified and security-conscious IT managed services provider, resulted in a mature information security program and significantly reduced information security risks for the Board. The accompanying chart shows the Board's maturity across a number of key security control areas, along with an estimate of their low initial maturity prior to this process to demonstrate their progress.

It was a big effort, Manuel acknowledged. "We were so far behind the times, catching up, working with staff on the new processes and their frustrations. We kept telling ourselves, 'It will be better in the long run.' And the staff now think that things are much better than they had been."



The maturity of Warren County DD Board's information security program shows significant improvements in key control areas from before their "five-year journey" to now.

Ratings: 0 = Non-existent Controls 4 = Controls are effective, managed, and measurable

As for how she feels now, Manuel shared, "I don't lose sleep over cyber. I trust Logan and GO Concepts, that they are handling it."

For his part, Stringer happily described no longer having to play "whack-a-mole" with IT issues. He is able to focus on forward-looking projects to improve efficiency and service delivery in the agency.

The experience of the Warren County DD Board is a success story for others to follow because they identified their limitations, recognized the need for expert partners who could provide the right technical and security capabilities, approached the transition as a multi-year process, and demonstrated the leadership's investment in the process.

Information Security Can Seem Overwhelming – Start by Doing the Basics Well

Before getting into the recommendations for basic security controls to prioritize, one key element needs to be in place:

Leadership Must Support Information Security

For information security efforts to be effective and taken seriously at any Board, they must have the clear support of the Trustees, Superintendent, and other leadership. This must be true both in communications and in budget decisions. Industry studies show that local government entities allocate less of their budgets to information security than their peers in other sectors. However, the example of the Warren County DD Board demonstrates that the right investments coupled with long-term commitment from the Superintendent can lead to better security, lower risks, and improved Board operations. With leadership support through planning, communications, and budgeting, these information security investments can be a win-win for the Board.

Stringer had this advice for his peers, based on the experiences of the Warren County DD Board: "For any county looking to do this, you need to have the Superintendent and management team invested and on board. It's a make-or-break for the project."

Basic Security Controls to Prioritize

An effective information security program executes the basic practices well, first and foremost. The myriad fancy tools and advanced techniques are useless without this foundation. Below we present a short list of recommended basic practices for any security program to prioritize. These recommendations are drawn from Eagle's years of experience in security risk advising and are based on industry best practices including the Center for Internet Security (CIS) Controls and other resources listed at the end of this document.

1. **Maintain an accurate inventory of IT hardware, applications used by the agency, and sensitive data sets.** Organizations cannot protect assets they don't know they have. This includes cloud applications and data transferred to Business Associates.
2. **Develop robust backup and disaster recovery capabilities.** In a ransomware attack or other significant incident, good backup and recovery can be the difference between a major disaster and just a tough day. Boards should follow industry best practices including multiple backups, at least one kept off-network, and regular restoration testing.
3. **Obtain insurance coverage that addresses the agency's information system risks.** Does the policy cover the right risks? Are the limits sufficient? Does the policy provide access to forensic specialists and other experts in a crisis? Are there any problematic exclusions, such as excluding cloud or third party hosted systems from coverage? At Eagle, we regularly see policies which on the surface seem

appropriate to an organization's needs, but upon closer reading have significant gaps. The devil is very much in the details.

4. **Conduct regular security risk assessments.**
   Regular assessments and an ongoing risk management process will identify the primary risks to an organization's information systems, quantify the financial impacts of worst-case scenarios, provide prioritized recommendations, and guide efforts to reduce risk over time. Failure to conduct risk assessments is itself a major risk.
5. **Implement endpoint protection and malware defenses.**
   Use top-tier, centrally managed anti-malware software that provides continuous monitoring, alerting, and next-generation defenses on all workstations and servers. Consider first the vendors on Gartner's Magic Quadrant for Endpoint Protection Platforms, though well-respected smaller organizations, such as Ohio's own Binary Defense, can also be excellent options.
6. **Engage in continuous vulnerability management.**
   Vulnerabilities in operating systems and software applications are common means of attack for malicious actors. Vulnerability management includes a robust and timely patch management program for IT assets and applications along with appropriate technical vulnerability scans to assess patching effectiveness and identify other network vulnerabilities for remediation.
7. **Provide security awareness training to staff.**
   Employees can be a weak point in an organization's security by clicking malicious links or attachments to give attackers access to the network. Or they can be an integral line of defense. Use regular, engaging security awareness training along with periodic assessment of employees through simulated phishing campaigns.
8. **Establish secure configurations for key systems.**
   Out of the box operating systems and applications are configured for ease of use rather than security. Establishing standardized secure configurations prevents attackers from taking advantage of open settings and vulnerable services. Industry standard configuration guides include the CIS Benchmarks and the Microsoft Security Compliance Toolkit. For smaller agencies, simplified guides are available such as the CIS Microsoft Windows 10 Cyber Hygiene Guide.
9. **Control use of administrative privileges.**
   Attackers often try to gain administrative privileges to spread across the network and access sensitive systems. Restrict the number of users with administrative privileges to workstations, servers, domains, and sensitive applications.
10. **Encrypt devices, file systems, and databases.**
    Don't let an intrusion or a lost device turn into a data breach. Enable full disk encryption on all laptops, mobile devices, workstations, and servers. Encrypt databases and sensitive folders in file systems wherever possible. Attend to best practices with management of the encryption keys.
11. **Monitor information systems security.**
    The average time to detect a breach is greater than six months, according to industry assessments. This is due to poor or nonexistent information systems monitoring. Board leaders should ask themselves, "If we had a breach, how would we even know?" Information system monitoring encompasses a variety of activities. Like many of the items on this list, most Boards will have a better experience contracting an expert organization rather than trying to accomplish this in-house.

Don't Go It Alone – Find Experts and Examples

The question in most leaders' minds when they see a list of security controls like the recommendations above is, "How can we possibly do all that?" The answer for most small and medium county DD Boards is that they will have the best chance of success by partnering with experts. We recommend two types of expert partners:

An information security risk and compliance advisor. Information security, risk management, and regulatory compliance are broad fields that require an array of expertise. A single risk assessment, for example, requires understanding of information security policies, management processes, compliance, asset management, digital communications, physical security, insider threats, external threats, technology best practices, software configuration, disaster recovery, and third-party risks, just to name a few. Quality advisors will measure where a Board stands, recommend and prioritize improvements, and help the Board develop and follow through on risk management plans.

An IT managed service provider. A quality IT managed service provider will have the expertise with IT security and regulatory compliance necessary for DD Boards and be able to implement most of the recommendations above. Any IT service contracts should specifically include the above security controls in the scope of work. Additionally, Board leaders need to validate that their IT contractors can and do implement these security controls.

For both of these partner recommendations, the reasoning is the same: by turning to trusted partners who specialize in security risk advising or IT services, the Board doesn't need to waste resources trying to reinvent these capabilities and can instead focus on its core mission of providing services to its community.

In conclusion, cyber threats to DD Boards have never been higher than they are right now. Superintendents and Board leadership have a responsibility to make the right investments in information security for their organizations. Fortunately, if done well, these provide tangible operational and financial benefits in addition to risk mitigation. Although information security is complex and overwhelming, Boards can experience major improvements by just doing the basics well, such as the recommendations provided here. Finally, Board leaders do not have to solve these challenges alone. They can make the greatest progress by partnering with experts and following the examples that others have provided.

At Eagle Consulting Partners, we specialize in information security, risk, and compliance advising for Ohio county Boards of Developmental Disabilities. We would be thrilled to work with your agency on the challenges addressed in this white paper. Please contact us at 216-503-0333 or eagleconsultingpartners.com/dd-boards to begin the conversation.

Additional Resources

Center for Internet Security (CIS) - https://www.cisecurity.org/

- CIS Controls: 20 foundational and advanced cybersecurity actions, where the most common attacks can be eliminated.
- CIS Benchmarks: Proven guidelines will enable you to safeguard operating systems, software and networks that are most vulnerable to cyber-attacks.
- CIS Controls Implementation Guide for Small- and Medium-Sized Enterprises (SMEs)
- CIS Controls Microsoft Windows 10 Cyber Hygiene Guide
- CIS Controls Telework and Small Office Network Security Guide
- Public Sector Cyber Defense Guide

National Institute for Standards and Technology (NIST) -
https://www.nist.gov/topics/cybersecurity

- NIST SP 800 Series Special Publications, especially 800-30 and 800-53
- NIST Cybersecurity Framework (CSF)
- NIST Risk Management Framework (RMF)
- NIST Computer Security Resource Center
- Small Business Information Security: The Fundamentals (NISTIR 7621)

Eagle Consulting Partners would like to thank Superintendent Megan Manuel and IT Manager Logan Stringer for allowing us to profile Warren County Board of Developmental Disabilities (https://warrencountydd.org/) in this white paper and for sharing their experiences with us. Eagle would also like to thank CEO John Gambill, Jr., and Director of Technical Operations Chris Pawel of GO Concepts (https://www.itfordd.com/) for their contributions.

About Eagle Consulting Partners

Eagle Consulting Partners has extensive experience supporting public and private organizations that serve the developmentally disabled. Eagle has worked with Ohio DD Boards, group homes, private agencies, and Special Olympics International. Eagle has particularly deep experience with Ohio's County Boards of Developmental Disabilities and has served more than 70 of the boards in numerous ways over the last 17 years.

Eagle's Services Include:

- **Computer Security Risk Assessment** which identifies risks, provides recommended courses of action, and prioritizes the risks that are the most urgent.
- **Privacy and Security Policies and Procedures** customized to the needs of Ohio County Boards of Developmental Disabilities and compliant with HIPAA, FERPA, IDEA, Ohio Revised Code, and Ohio Administrative Code
- **Risk Management Support** to assist in implementing security measures identified in a risk assessment or policy engagement.
- **Privacy Risk Analysis** of risks related to paper records and oral PHI in an organization
- **Technical Vulnerability Analysis** of the perimeter and interior of the network
- **Disaster Recovery Planning**
- **Data Breach Response**
- **Policy Gap Analysis**
- **HIPAA Compliance Audit**
- **HIPAA Training**
- **Employee Security Awareness Training**
- **Other HIPAA-related services**

More information is available at eagleconsultingpartners.com/dd-boards, or contact us at 216-503-0333.

About the Author

Mike Owens specializes in helping government agencies, healthcare organizations, and Business Associates protect the people they serve through risk analysis and information security consulting. He provides HIPAA security risk analysis, ongoing risk management and information security support, computer security awareness training, policy and procedure support, disaster recovery planning, and project management services. He has been with Eagle Consulting Partners since 2017. A graduate of Georgetown University, he holds a certification in CompTIA Network+.

[i] Source: https://blog.emsisoft.com/en/34193/state-of-ransomware-in-the-u-s-2019-report-for-q1-to-q3/
[ii] Source: https://warrencountydd.org/
[iii] This is not an endorsement. Eagle has no business relationship with GO Concepts.
Cover Image by rawpixel from Pixabay. Other images from Pixabay and Vecteezy.