## Comprehensive IT Solutions

## Your Guide to Efficient Network Management and Reliable User Support

CyberKrush

**Ready to go from  “Zero to Hero”**

## Network Management

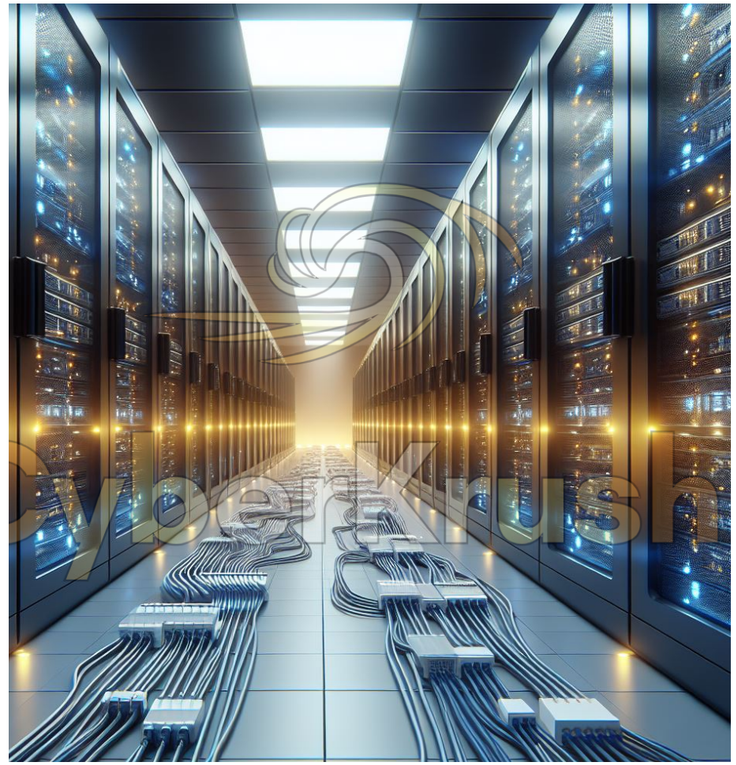
**At the core of every successful business lies a robust network infrastructure. Our network management services ensure:**

- **Preventative Issue Resolution**
- **Customizable Scalable Solutions**
- **Network Performance Optimization**

## Server Administration

**Efficient server administration is the backbone of a stable IT environment. Our services include:**

- **Server Setup Maintenance**
- **Security Patching Maintenance**
- **Backup Recovery Solutions**
- **Server Optimization Services**



## Security Enhancements

Protecting your data and infrastructure from cyber threats is paramount. Our security enhancements encompass:

- Security System Implementation
- Security Audit Assessment
- Cybersecurity Training Programs

## User Support

Empowering your employees with reliable technical support is essential for smooth operations. Our user support services offer:

- IT Helpdesk Support
- Remote Troubleshooting Support
- Customized Support Plan

## Contact US!

Email: barryk@cyberkrush.com
Phone: 724-689-2063
Website:  https://cyberkrush.com/

Trust our experienced team to manage your IT infrastructure effectively, so you can focus on what matters most—growing your business.

Let us be your partner in achieving IT excellence.

# Barry Kimmell

Contact Information: barryk@cyberkrush.com , (724) 689-2063

## Summary

I am an Independent Consultant/Free Lance Information Security Professional and founder of CyberKrush LLC with over 14 years of experience conducting threat assessments, vulnerability assessments, and risk assessments for the United States Navy, and additional private sector experience for Draper, Raytheon, National Grid and Hanscom Federal Credit Union, and BAE**.**

## Professional Experience:

**Independent Consultant** 06/2020 – Current

- Help organizations with various frameworks to include ARS, CMS, ISO 27001, RMF, and briefly CMMC (crosswalk)
- Help organizations with policy review, gap assessments, make recommendation based on findings, develop policies based around the RMF requirement 800-37
- Help organizations go from "0 to hero" with an average 2–3-year ATO outcome
- Help organizations with all aspects of eMASS to include but not limited to the Controlexport and TRexport
- Ensure organizations have a full understanding of what is "required" to include giving guidance on how to get become compliant based on their required framework
- Help with technical pieces of their system is needed:
    - Setting up and maintain back up drives
    - Provisioning/Deprovisioning accounts
    - Setting up OUs on the network
    - Defining what GPO to enforce and setting them
    - Installing/removing software
    - User Troubleshooting
- Manage multiple IT Projects to ensure successful delivery within budget and timeline
- Manage budget in excess of 2 million dollars
- Conduct regular project status meetings and provided progress updates to key stakeholders.
- Collaborate with vendors and external partners to coordinate project activities and ensure seamless integration of services.
- Monitor project budgets and expenses, tracking and controlling costs to meet financial targets.

**Abilene Christian University**
*Course Developer/Adjunct Teacher* *01/2020 – Current*

- Utilize variety of technologies and instructional methodologies to keep courses fresh and engaging.
- Help students develop talent through range of exercises readings and discussions.
- Lead Adjunct for several under-graduate Cybersecurity courses
    - ITA 460 Project Management for IT
    - ITA 475 Risk & Incident Plan & Responses
    - ITO 310 Intro Computer and Info Security
    - ITO 473 Cybersecurity Policy

**BAE Systems**
*Manager, Information Security* *07/18-12/2020*

- Work with technology **leadership** to **develop, plan, implement** and provide oversight of an enterprise security program and roadmap
- Analyzing and preparing reports for management on team goal achievement, workflow, p roductivity and performance
- Create and maintain **security architecture artifacts** that can be used to leverage security capabilities in new initiatives and operations
- Analyzes and prepares reports for management on team goal achievement, workflow, pro ductivity and performance
- Directs day-to-day workflow and site management of team and associates
- Engage with the information security program management team to ensure that projects a re scoped and designed in alignment with architecture models.
- Raise awareness and adherence to secure development practices on development teams
- Using a **risk management approach**, negotiating risk levels and response
- Execute strategies to align department with business objectives and division goal
- During yearly SVA with DCSA scored a "**Superio**r" rating.
- Knowledge of development and implementation of GPOs, Server hardening and Microso ft Clustering technologies
- Manage **Splunk** user accounts (create, delete, modify, etc.)
- Manage all aspects of information systems security as it applies to the SCI, SAP, and DoD community (NISPOM, NIST 800-37, NIST SP 800-53).

**The Charles Stark Laboratory**
*Sr. Risk Manager/ Security Engineer* *11/17-07/18 (Contract)*

- Provided system security support to Strategic Programs at Draper. Ensures all systems are compliant with all DISA STIG administrative and technical requirements.

- Performs appropriate continuous monitoring and systems security testing and provides mitigation solutions for identified findings and patching requirements.
- Ensured that proposed system changes are reviewed and that implemented system modifications do not adversely impact the security of the system.
- Provided guidance for Computer Security needs based on the National Industrial Security Program Operating Manual, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), Navy RMF, and Draper Policy and Procedures Manual for all levels of management and technical staff.
- Responsible for inspection and revision of system plans for each accredited system. Documents changes to system plans and special security requirements as needed, and communicates these changes to Management Provides day-to-day support to the adherence of policies, procedures and best practices.
- Prepared and wrote individualized and specialized system security plans for approval. Reviewed and revised these plans based upon the analysis/interpretation of the system components and the processing needs/objectives of each individual system custodian and user.
- Developed component and physical architectures in collaboration with IT and the business to enable security-by-design that balances risks and opportunities for Draper Labs.
- Developed and implemented GPOs, Server hardening and Microsoft Clustering technolog ies

**Hanscom Federal Credit Union** *07/17 – 11/17*
*Information Security Risk Manager*

- Develop and organize standard toolkits and tool development repositories, and custom content within **Splunk.**
- **Ensured compliance in Business Continuity Planning, Incident Response Planning, and Risk Assessments across 13 branches.**
- Coordinate training and testing, tracks testing recommendations until completion, and updates the plan as needed to ensure compliance.
- **Performed annual business continuity planning, training, and testing which results in employees becoming more familiar with cyber security risks.**
- Coordinated with IT disaster recovery program and track test results.
- **Developed metrics and risk tolerance from credit union's risk appetite statement.**
- Performed risk management reporting for the Risk Management Committee and Board.
- **Reviewed and consider new third-party vendor technology products, this lead to partnering with Knowbe4 for cyber awareness and Quantivate to help manage our Enterprise Risk Management, Business Impact Analysis, and vendor management.**

**National Grid** *12/16 – 07/17 (Contract)*
*Cyber Security Incident Manager/Business Continuity Planner*

- **Served as the Lead Cyber Security Incident Manager (CSIM) for a group of four personnel that led efforts across ITS including determination the criticality of an incident, appropriate containment, and mitigation activities.**
- **During an active incident response, prioritize advanced computer and network forensic investigations relating to various forms of malware, computer intrusion, theft of information, denial of service, data breaches, etc.**
- Developed contingency plans to deal with organizational emergencies.
- **Managed the Cyber Incident Response Retainer Service on behalf of the CISO and recommend activation for incidents where assistance is required.**
- Developed the disaster recovery plans for physical locations with critical assets such as data centers.
- **Developed emergency management plans for recovery decision making and communications, continuity of critical departmental processes, or temporary shut-down of non-critical departments to ensure continuity of operation and governance**
- Supported the alignment between the Disaster Recovery and Business Continuity programs and Cyber Security Incident Response, including participation in Disaster Recovery testing activities.
- **Managed the alignment of ITS CSIR programs with other areas of groups to include: strategy, governance, risk and compliance, disaster recovery and business operations.**
- Acted as the lead for table-top exercises, which assess the effectiveness of cyber incident response capabilities across people, processes, and technology.
- Prepared reports summarizing operational results, financial performance, or accomplishments of specified objectives, goals, or plans.

**Raytheon** *08/16 – 12/16 (Contract)*
*Senior Cyber Information Assurance Specialist I*

- **Managed all aspects of information systems security as it applies to the SCI, SAP, and DoD community (NISPOM, NIST 800-37, NIST SP 800-53).**
- Develop and organize standard toolkits and tool development repositories, and custom content for log remediation within **Splunk.**
- **Assisted the Information System Security Officer (ISSO) on preparing the Information System Security Plans, Protection Profiles, etc.**
- Worked with GRC platforms to help in the guidance of finding gap analysis, risk analysis, and IT auditing.
- Worked closely with local DSS, ODAA, and other government approval authorities to achieve system accreditation and maintain compliance for all collateral classified information systems.
- **Conducted regular AIS audits to ensure accredited systems are being operated securely and computer security policies and procedures are implemented as defined in security plans.**
- Provided technical and user support for numerous standalone and network systems to include routine backs-ups, virus updates, patches, service packs, and hot fixes, set-up of

user accounts, password resets, adding/removing hardware and ensuring all secure related documentation is notated as required.

- **Supported the assessment and mitigation of system security threats and risks throughout the program life cycle which was based around the DoD RMF process 1-6.**
- **Implemented site procedures for marking, handling, and controlling, removing, transporting, sanitizing, reusing, and destroying media/equipment containing classified information, this in returned helped when it came time for inventory as easy way to identify what assets we had on hand.**

**United States Navy**

*Information Assurance Office/Instructor* *01/13 – current*

- **Ensured Information Security and availability by conducting threat assessments, vulnerability assessments, and risk assessments.**
- Continually assess risk on network security posture before and after corrective actions taken.
- **Utilized the NISPOM chart to help in the decision scoring of vulnerability, subsequently assisting in assigning mitigation to the vulnerability.**
- Maintained and provide daily client support to over 200 Tier 1 end users on 113 workstations and 3 CISCO VoIP phones by ensuring the Confidentiality, Integrity, and Availability of network information.
- Investigated internal security violations that occur on networks
- **Ensured proper chain of custody logs were filled out to ensure the integrity was not compromised.**
- Implemented a DoD-wide Public Key Infrastructure (PKI) to maintain the digital certificate life cycle, including issuance, suspension, and revocation. Processed system authorization access request for NIPR and SIPR networks. Audited user files for inappropriate access levels and protection from cyber-attacks.

*Military Police Officer* *06/04 – 08/2012*

- Supervised security dispatch center for various NAS Naval Station over a 12 year period containing roughly 2,500 personnel at any given time.
- Used an array of specialized criminal investigative techniques to resolve investigations. Prepared reports of investigations and criminal intelligence reports detailing diverse contributing causes. Testified in administrative proceedings and court hearings
- Investigate possible security breaches while conducting physical security checks to includes recommending mitigations
- Analyzed and evaluated information to determine the appropriate course of criminal prosecution

- Identified, collected, and seized documentary or physical evidence; processes crime scenes; assisted with interviews of witnesses and suspects.
- Interviewed subjects, targets and witnesses for information verification and corroboration
- Verified and authenticated the validity and admissibility of evidence and preserved its integrity for court hearings

**Clearance**

Active TS/SCI Clearance

**Education**

BS in Cyber Security- University of Maryland University College
MS in Cyber Security Management- University of Maryland University College

CyberKrush, LLC
Barry Kimmell, Founder
barryk@cyberkrush.com
724-689-2063
UEI:  URLUJJ5X9L33
Cage Code: 9FM93

CyberKrush

# Past Performance

Over the past few years, CyberKrush, LLC has consistently demonstrated its commitment to effective risk management by implementing a robust framework. This framework has enabled us to proactively identify, assess, mitigate, and monitor risks across various projects and initiatives. Our accomplishments in this area have significantly contributed to our overall success and helped us maintain a strong position in the market. Here are some key highlights of our past performance in risk management:

1. Comprehensive Risk Identification: We have successfully developed a systematic approach to identify risks at every stage of our projects. Our teams have actively engaged stakeholders, conducted thorough analyses, and utilized various risk identification techniques to identify and document all potential risks. Doing so has minimized the chances of unexpected events impacting our projects negatively.
2. Rigorous Risk Assessment: Our organization has excelled in conducting comprehensive risk assessments once risks are identified. We have employed various qualitative and quantitative methods to assess the impact and likelihood of each risk. By assigning appropriate risk scores, we have prioritized our efforts and resources towards addressing the most critical risks first, ensuring effective risk mitigation.
3. Proactive Risk Mitigation: We have implemented proactive risk mitigation strategies to minimize the impact and likelihood of identified risks. Our organization has developed contingency plans, alternative methods, and risk response plans for each significant risk. We have prevented potential disruptions by addressing risks at their root causes and consistently met project objectives.
4. Robust Risk Monitoring: Our risk management framework includes a dynamic monitoring process to track identified risks continuously. We have established key risk indicators (KRIs) and implemented regular monitoring mechanisms to identify any changes in risk levels. By closely monitoring risks throughout the project lifecycle, we have been able to adapt and respond promptly to emerging threats.
5. Continuous Improvement: Our commitment to constant improvement in risk management is evident through our post-project reviews and lessons-learned sessions. We actively seek stakeholder feedback, analyze project outcomes, and update our risk management practices accordingly. This iterative approach has allowed us to continually enhance our risk management framework and adapt to new challenges and emerging risks.
6. Recognition and Compliance: External auditors and regulatory bodies have recognized and commended our risk management framework. We have consistently demonstrated compliance with industry best practices, standards, and regulations, giving our stakeholders confidence in our risk management capabilities.

Our past risk management performance reflects our organization's dedication to proactive and effective risk management practices. By consistently implementing our risk management framework and achieving these accomplishments, we have positioned ourselves as a reliable and

resilient organization capable of navigating complex challenges while ensuring the successful delivery of our projects.

## Recent Accomplishments: Achieving Authorization to Operate (ATO) using the Risk Management Framework (RMF)/ Federal Information Security Moderization Process

### FRAMACO

In collaboration with FRAMACO, we successfully guided them through the RMF process to achieve Authorization to Operate (ATO) for their critical system. We began by comprehensively assessing their security posture, identifying potential risks, and documenting the necessary security controls. Through workshops and close collaboration with FRAMACO stakeholders, we developed a robust System Security Plan (SSP) that addressed all required rules and aligned with industry standards and regulatory requirements.

Next, we assisted FRAMACO in implementing and integrating the necessary security controls into its system architecture. This involved establishing appropriate access controls, implementing continuous monitoring mechanisms, and ensuring secure configuration management practices. Our team provided expertise in effectively selecting and deploying relevant security tools and technologies to bolster their security posture.

To ensure compliance with the RMF process, we facilitated thorough security testing and evaluation, including vulnerability assessments and penetration testing. By conducting these assessments, we identified and addressed potential vulnerabilities and implemented appropriate remediation measures to enhance the system's overall security.

FRAMACO compiled all necessary artifacts through our guidance and support, including security assessment reports and contingency plans. We worked closely with them to document and justify deviations from standard security controls, ensuring a comprehensive and well-documented package for the authorization review.

Finally, we assisted FRAMACO in preparing for the ATO review board by providing detailed briefings and facilitating the necessary discussions. Our team addressed any concerns or questions raised by the review board, ensuring a smooth and successful authorization process. As a result of our collective efforts, FRAMACO achieved a **2-year** ATO, enabling them to operate their system while maintaining high security and compliance confidently.

## SkyWater Technologies

For SkyWater Technologies, CyberKrush, LLC provided extensive support in their journey to obtain an ATO using the RMF process. Our engagement began with thoroughly assessing their system's security posture and identifying potential risks and vulnerabilities. Through collaboration with their internal security team, we facilitated the developing of a comprehensive SSP encompassing all necessary security controls.

We worked closely with SkyWater Technologies to properly implement identified security controls and integrate safe practices within their system architecture. This involved assisting in establishing robust identity and access management processes, implementing security monitoring and incident response capabilities, and conducting security awareness training for their personnel.

To validate the effectiveness of their security measures, we conducted rigorous security testing and evaluation, including vulnerability scanning and penetration testing. Our team provided recommendations for remediation and guided SkyWater Technologies in implementing the necessary fixes to enhance their system's security posture.

Throughout the process, we supported SkyWater Technologies in the creation of required security artifacts, including security assessment reports, contingency plans, and incident response procedures. We ensured that all documentation adhered to the RMF guidelines and satisfied the expectations of the authorization review board.

We conducted thorough briefings and readiness assessments as the ATO review approached to prepare SkyWater Technologies for the review board's inquiries. Our team addressed any concerns or questions raised during the review, ensuring a comprehensive understanding of the security controls implemented.

Thanks to our collaborative efforts, SkyWater Technologies obtained a **2-year** ATO, affirming their security measures' effectiveness and commitment to maintaining a secure environment for their systems and data.

## Haigh Farr

Our involvement with Haigh Farr centered around guiding them through the RMF process and supporting their efforts to achieve an ATO for their critical system. We initiated the engagement by conducting an in-depth assessment of their existing security posture, identifying potential risks and vulnerabilities. Based on this assessment, we collaborated with Haigh Farr team to develop a robust SSP that addressed all required security controls and aligned with industry best practices.

We provided comprehensive guidance and expertise to Haigh Farr in implementing and integrating the necessary security controls into their system architecture. This involved establishing secure network boundaries, implementing strong access controls, and deploying monitoring solutions for enhanced threat detection and incident response capabilities.
To ensure the effectiveness of their security measures, we conducted thorough security testing and evaluation, including vulnerability assessments and penetration testing. Through these assessments, we identified and addressed potential vulnerabilities, enabling Haigh Farr to enhance its system's overall security.

Our team worked closely with Haigh Farr to compile all necessary artifacts, including security assessment reports, contingency plans, and incident response procedures. We assisted them in documenting deviations from standard security controls, ensuring transparency and compliance with the RMF process.

As the ATO review approached, we conducted extensive briefings and mock review sessions to prepare Haigh Farr for the authorization review board's scrutiny. Our team addressed any concerns or questions raised during these sessions, ensuring Haigh Farr readiness for the review.

Through our collaborative efforts, Haigh Farr achieved a **3-year** ATO, validating their security measures' effectiveness and commitment to maintaining a secure operating environment. Their successful accomplishment demonstrates their dedication to robust risk management practices and adherence to the RMF process.

## BAE Systems

1. System Categorization: Assisted BAE Systems in determining the appropriate categorization of their geospatial systems according to the RMF. This step involved assessing the potential impact on the organization and defining the necessary security controls accordingly.
2. Security Control Implementation: Collaborated closely with the team at BAE Systems to identify and implement the specific security controls required for their geospatial systems. These controls were carefully selected to address geospatial data's unique challenges and risks.
3. Continuous Monitoring: Worked hand in hand with BAE System to establish a robust continuous monitoring program for their geospatial systems. This involved developing processes and tools to detect and respond to potential security incidents in real time, ensuring prompt mitigation of any threats.
4. Documentation and Compliance: We supported [Organization's Name] in generating the necessary documentation to demonstrate compliance with the RMF requirements. This included preparing system security plans, conducting security assessments, and maintaining an accurate and up-to-date record of their geospatial systems' security posture.

By overseeing the entire IT infrastructure, including the geospatial systems, we ensured a holistic approach to security. This approach allowed us to identify potential vulnerabilities and implement appropriate controls across the organization's technology landscape. This infrastructure included 100 networked desktops, four servers, and two backup devices for continuity.

Through our collaborative efforts, BAE System has maintained high security for its geospatial systems while aligning with the RMF guidelines. We are confident that our ISSM support will continue to strengthen their security posture and enable them to leverage their geospatial infrastructure confidently.

## Draper Laboratory

As the Information System Security Manager (ISSM) for Draper Laboratory, I oversaw and implemented robust security measures to safeguard the critical information systems supporting ballistic missiles. In this role, I work diligently to ensure the confidentiality, integrity, and availability of classified data while adhering to stringent government regulations and industry best practices. By conducting thorough risk assessments, developing comprehensive security policies and procedures, and implementing advanced cybersecurity technologies, I strive to create a secure environment that mitigates the potential risks and threats to our information systems. Furthermore, I collaborate closely with stakeholders, conduct regular security audits, and provide continuous training and awareness programs to foster a culture of security consciousness among our personnel. With an unwavering commitment to the highest standards of security, I am dedicated to ensuring the protection and reliability of our vital information systems that support the critical mission of ballistic missile defense.

## Aerojet Rocketdyne

CyberKrush, LLC has a proven track record of effectively managing risks within the Secret Internet Protocol Router Network (SIPRNet) by implementing a robust Risk Management Framework (RMF). Our accomplishments in this area have been instrumental in safeguarding sensitive information and maintaining the integrity, confidentiality, and availability of the SIPRNet. Here are some key highlights of our past performance in risk management specific to the SIPRNet:

1. Thorough Risk Identification: We have demonstrated expertise in identifying risks specific to the SIPRNet environment. Our team has conducted comprehensive risk assessments, considering unauthorized access, data breaches, malware attacks, insider threats, and physical security vulnerabilities. By proactively identifying and documenting these risks, we have been able to implement appropriate controls and mitigation strategies.

2. Rigorous Risk Assessment: Our organization has performed thorough risk assessments for the SIPRNet to evaluate the potential impact, likelihood, and severity of identified risks. We have employed qualitative and quantitative analysis methods, utilizing industry best practices and standards. This has enabled us to prioritize our efforts and allocate resources effectively for risk mitigation.
3. Effective Risk Mitigation Strategies: Through our RMF process, we have implemented effective risk mitigation strategies to protect the SIPRNet. We have established robust access control mechanisms and implemented multifactor authentication, encryption protocols, and intrusion detection and prevention systems. Additionally, we have developed and enforced stringent security policies and procedures, including regular security awareness training for authorized users to mitigate the risk of insider threats.
4. Continuous Monitoring and Incident Response: We have implemented comprehensive monitoring mechanisms to detect and respond to potential risks and security incidents within the SIPRNet. This includes constant monitoring of network traffic, system logs, and security event management systems. By promptly identifying and responding to anomalies and security incidents, we have minimized the impact of potential threats and vulnerabilities.
5. Compliance and Certification: Our risk management framework for the SIPRNet aligns with the necessary security requirements and standards. We have maintained compliance with relevant regulations, including Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and National Institute of Standards and Technology (NIST) guidelines. Our organization has undergone regular audits and assessments to ensure adherence to these standards, providing confidence in the security of the SIPRNet.
6. Incident Analysis and Lessons Learned: In the event of security incidents, we have conducted thorough incident analysis and lessons learned sessions. Our team has investigated the root causes of incidents, identified areas for improvement, and updated security controls and procedures accordingly. This iterative approach has allowed us to continuously enhance the security posture of the SIPRNet and mitigate future risks effectively.

Overall, CyberKrush, LLC past performance in risk management for the SIPRNet demonstrates our organization's commitment to safeguarding sensitive information and ensuring the integrity of this critical network. Through the implementation of a robust Risk Management Framework, we have consistently identified, assessed, and mitigated risks specific to the SIPRNet, contributing to its secure operation and trusted communication capabilities.

## Closing

Partnering with CyberKrush, LLC will give you peace of mind, knowing that your system's security is in capable hands.

Furthermore, the owner of CyberKrush, LLC is an esteemed Cybersecurity adjunct for Abilene Christian University. With this unique affiliation, our team deeply understands the specific challenges and requirements within the academic sector. We bring a wealth of knowledge and insights from working closely with Abilene Christian University, enabling us to tailor our Annual Assessments to meet the specific needs and regulatory frameworks commonly encountered in educational institutions. This valuable association further reinforces our commitment to excellence and alignment with industry standards. By engaging with CyberKrush, LLC, you can leverage our comprehensive expertise and benefit from our unique insights into the cybersecurity landscape of educational institutions.

We look forward to the opportunity to collaborate with you and contribute to the success of your cybersecurity efforts.

Cheers,
BarryK