Approach to Digital Security

North Deanery Technology Office

Immaculate Heart of Mary Parish and School

Christ the King Parish and School

St. Andrew the Apostle Parish

St. Joan of Arc Parish and School

St. Lawrence Parish and School

St. Luke the Evangelist Parish and School

St. Matthew the Apostle Parish and School

St. Pius X Parish and School

St. Simon the Apostle Parish and School

St. Thomas Aquinas Parish and School

Bishop Chatard High School

May 3, 2019

Thomas Groot
CIO, North Deanery

N D

North Deanery
Technology Office

Introduction

Securing our digital assets and protecting our staff and students is the highest priority for the North Deanery Technology Office. The Tech Office works with our parishes and schools to improve their security posture. This includes many areas of concern:

- *Physical safety systems* that provide physical access control to the facility, security video, and operational management systems for the school
- *Data networking* that is secure from unauthorized use to protect our computing and storage assets
- *Internet access* by staff and students that is safe and protected from malicious attack
- *Information security* that maintains staff and student data privacy in compliance with Federal and State law
- *Identity management* to provide secure access to a wide array of systems for students and staff
- *Incident management* processes used to respond to security events

Digital security is a wide-ranging, complex and technically demanding field. Our areas of concern are intertwined, requiring a holistic approach to design and decision making.

Digital security is fundamentally a matter of risk management, involving tradeoffs of cost and benefits. Our risks are never reduced to zero. The landscape of threats is constantly evolving, driven by the pace of technology development and the evolving methods of cyber criminals.

This document describes our approach to digital security. It explores the reasons why this is a top priority and outlines the key areas of focus for our investments of time and money. Its purpose is to raise awareness of the breadth and scope of our concerns with digital security. We need alignment on our direction to ensure that our campuses are safe for our staff and students.

Threat Landscape

It’s important to begin with an understanding of the threats we face every day. They are significant and immediate.

We tend to think of ourselves simply as Catholic schools and parishes in Indianapolis. However, the digital world knows no boundaries, and we are exposed to a global array of actors and threats.

Closest to home are current and former employees and students, who have access to our network and applications and knowledge of our operations. Statistically, this is the group with the highest probability of causing damage to our digital assets. This threat may be intentional, such as a malicious attack, or unintentional, such as accidental deletion of data.

We also face actors with criminal intent. This threat includes local and regional criminals seeking financial gain through theft of property or information. We also face the possibility of individuals or groups that intend to harm students, staff, or the reputation of the school or Church. These threats may be a combination of physical action on campus and assault on campus digital systems. As our schools have become more dependent on technology to function, damage to the digital platform can quickly impact school operations. It is wise to consider physical security and digital security in relation to each other today.

We are directly exposed to criminals at a global level due to our use of Internet resources. This is a wide-ranging and growing threat. Hackers anywhere in the world can reach our campuses. Terror and criminal organizations use the Internet for extortion and income generation. Many state actors are active in cyber-espionage, income generation, and politically-motivated data collection. Some of these actors are highly sophisticated, with far deeper knowledge of cybersecurity and far greater resources than we have at our disposal.

These actors can reach us over our Internet connections, through e-mail, and on our cloud-hosted systems. As a group, they are known to target small organizations such as schools due to their lower security capabilities and lack of readiness for cyber-attack. A school is an easy target compared to a large corporation, with a higher likelihood of a successful outcome for the attacker.

Why would a cybercriminal be interested in one of our schools? Attackers may seek one or more results including:

- Control of computing resources to repurpose for crypto-mining or botnets
- Confidential information about staff or students to sell or use for other criminal purposes
- Hijacked email accounts to use for spam mail or other purposes
- Cash payments obtained through fraud or ransom
- Control of security systems to support an on-site attack
- Access to financial systems for fraud and theft
- Vandalism to damage property or to attack students or teachers
- Damage to the reputation of the school or parish, such as through Web site hacking

Attacks such as these happen every day at Bishop Chatard and on other North Deanery campuses. Their frequency seems to be growing. Here are a few recent examples to consider:

- Every deanery campus has its Internet connection scanned thousands of times every day by malicious actors. We have firewalls in place at every Internet boundary to prevent these attacks from reaching internal resources.
- Phishing attacks are a common occurrence on every campus and have been for the last several years. We see a growing frequency of these attacks. Attackers launch email, text messages, and phone calls to staff, attempting to gain account credentials, banking account numbers, and cash payments. In the last year Bishop Chatard has experienced phishing attacks targeting our school, impersonating the President and Principal and asking staff members to purchase gift cards for the criminal. This type of fraud attack is occurring in most schools and small businesses today.
- Two years ago, a deanery school experienced a successful ransomware attack. The school lost all of its servers and some staff computers in the attack, requiring new equipment to be purchased and restored from backups.
- Staff accounts at Bishop Chatard and other deanery schools are hacked and taken over by attackers. These accounts can normally be recovered by system administrators, but personal information may be stolen, and stored files may be lost. This happens a few times per year in the deanery. The most common cause is weak passwords on the accounts.
- A deanery school had a tech-savvy student launch a virus program on its internal network as an act of malicious vandalism. The school spent considerable time cleansing the malware from its computers.

Everyone is aware of the risks that accompany our emerging digital culture. We deal with these risks in our personal lives as well as at school. The news is filled with stories of massive data theft, cyber warfare, and issues with social media. We seem to hear a new horror story every week.

As Catholics, we approach the world as it is and move forward with our mission. Jesus says, “Be not afraid.” We try to be clear-eyed about the risks we face, and to deal with them as best we can. Our hope is in the Lord, and we trust in his divine Providence. Understanding our threats should motivate fortitude, not fear and retreat. If we are diligent, we can maintain a safe learning environment in our schools with the resources we have been given.

Focus Areas

Our digital security approach is organized into six focus areas. These areas are a good match for the state of our deanery campuses today. This section identifies our six focus areas and provides some definition and approach for them.

Identity and Access Management

Access management is about controlling what users are allowed to do in a digital environment. This topic is focused on two questions:

- Is the person requesting access who they say they are?
- What is this person allowed to do?

Everyone is familiar with logging in to get access to a system. In fact, users cannot do anything on many systems until they log in. This makes identity management one of the most fundamental and critical components of digital applications. Users interact with identity management systems dozens of times in a typical day.

We use infrastructure components for authentication such as Active Directory and Google Directory Services. Processes for administering user accounts and access rights are critical. Capabilities such as data and network encryption depend on certificate services managed in these systems. Physical security systems such as door access card readers also depend on identity management data. By their very nature, identity management systems are one of the most sensitive and critical components in the digital environment and require strong security themselves.

Our focus is on maintaining simple, secure services for identity management. This includes internal processes on campus to manage user accounts and credentials effectively. We have a special concern for users with elevated or administrative privileges to systems – those accounts pose extra security risks and require extra oversight and controls.

Intrusion Detection and Prevention

This area concerns our digital line of defense against the threats outlined earlier. It includes some familiar components, such as antivirus/malware scanning and Internet content filtering. It also includes more confidential capabilities, such as tools to identify intrusions and capture information about them. We focus on these questions:

- How do we keep malicious actors out?
- How do we know if we are being attacked?

- Have our systems or data been compromised?

This is a complex and dynamic space driven by the evolving threat landscape. Partnership with first-class global vendors for tools, data, and processes is critical to success. Our partnership is primarily with Fortinet, a leading global supplier of cybersecurity products and services. Some of our schools are using Cisco Meraki as a support vendor.

Data Backup and Recovery

Having a strong data backup and recovery process addresses a multitude of threat exposures. Unintended data loss is one of the most common digital security incidents: consider users accidentally deleting important files. Recovery from a ransomware attack is much simpler with a complete, readily-accessible data backup available.

However, data backup procedures typically receive very little attention in most companies and schools. People store critical documents on their laptops with no backup copy. People assume their files are "in the cloud" and therefore are safe. Server backup processes go unmonitored for months, and then are discovered to have failed only when a backup copy is needed.

Our focus is on establishing robust processes and tools for data backup and recovery. Today this must address cloud storage as well as on-premises servers and user computing devices. We also consider data recovery for cloud-hosted applications on which our campuses depend. These processes are easy to ignore but require diligent attention. We are making them a priority in our digital security approach.

Data Stewardship and Governance

This topic concerns our oversight and management of data, especially confidential and private information about students and staff. We identify sensitive data in our systems, define lifecycles for that data including when it should be deleted, and define who has rights to edit and view the data.

Many people do not realize that Federal Title funding to schools (including non-public schools) requires us to comply with several Federal laws concerning student data privacy and Internet protection. Indiana state grants typically have data security requirements as well. If a school loses student data in a data breach, it puts all of the school's Federal funding at risk, and potentially much of its Indiana state funding as well.

Exercising responsible management of student and family data is also a matter of the reputation of the school in its community. Improper access of student information, or worse, its publication on the Internet, is certain to cause problems for the school.

Our work in this area primarily concerns data management processes and access rights. We also consider data migrations required by school processes that transmit sensitive student data between systems. Our goal is to minimize these transfers, and tightly control user access to sensitive data.

Security Incident Management

What steps should we take when a security incident occurs? What do we do if data is stolen, or a server is compromised, or someone responds to a phishing scam? This is the subject of incident management.

Our processes for digital security overlap with other safety processes on our campuses. Fire drills and school lockdown procedures are extensively managed in schools. Digital security incidents are similar, but they may also require in-depth technical expertise to resolve. A malware attack will require system administrators to take action to remediate damaged infrastructure, for example.

Our focus is on improving the preparedness of our campuses to respond to likely digital incidents. This includes documenting procedures, training staff, and developing vendor support relationships before an event occurs.

Security Awareness

We recognize that our staff and students are critical to the digital safety of our campuses. Their preparation and knowledge are very important. Raising their awareness of digital security and the security processes they support is a key goal of our program.

Our action on this topic includes ongoing communication about security risks, tools, and processes. Students need to understand their boundaries in their school's infrastructure. Staff need training to identify malware and phishing attacks. Everyone needs to understand how to gain access to the systems they need. We have formal training programs as well as ad-hoc resources that support this communication.

We approach this topic recognizing that it has personal benefits for people as well as benefits for the parish and school. Everyone is challenged today to be safe in personal online banking, social media, and email use. Many of the same digital safety techniques apply in personal life as in professional life.

Conclusion

Our digital security initiative is driving improvement in our North Deanery churches and schools, making them safer and more effective in their missions. Our six focus areas frame the work we are doing to accomplish the goal of a secure digital environment. We understand the evolving threat landscape that we face, and it motivates us to continue to focus on digital security as a top priority.

Our staff and students can expect ongoing change driven by the imperatives of digital security. As our risks change, our systems and processes must respond. The Tech Office will continue to lead our campuses through this change and is ready to help when challenges appear.