Forward Edge
The technology edge for education

CYBERSECURITY

MFA Taskforce Whitepaper

MFA Taskforce Evaluates Options for K-12 Districts

A whitepaper detailing extensive research done by a Forward Edge taskforce to give K-12 school districts a better understanding of different multi-factor authentication options and implementation strategies.

Read now

The Need, Our Purpose

COVID-19 flipped the world upside down and pushed every industry in the world into new directions. From manufacturing changes in processes as well as supply and demand, all the way to the education sector and the need to support remote education infrastructure for students. Due to rapid changes like this, we also saw a dramatic influx of cybersecurity threats hitting every industry, threat actors took advantage of these poorly implemented changes and left no industry unchecked. With little support or time to prepare for these technology changes, threat actors found easy targets worldwide and made easy exploits of those suffering from the effects brought on by the global pandemic.

Education was the least prepared and the easiest of targets given that it typically has the least amount of funding and technology support in comparison to other industries. Schools had to respond quickly to the pandemic changes and made huge efforts in converting and ensuring remote learning was possible. Unfortunately and unsurprisingly, schools had significant gaps in security and the resilience of their organization's infrastructure. Education deals with personal information every single day, like student records including health information. Also, combining the urgency to implement remote learning, what missed steps or shortcuts were taken to make sure remote learning was possible? What better target for threat actors than organizations with limited security posture and exploitable records?

Because of the nature and obvious threats of cybercrime, our concerns were focused on schools and assisting in reassessing their technology and state of security, one of which being cybersecurity insurance. In cases of cybercrime, schools want to make sure they are insured if ever targetted or exploited by a threat actor. Their insurance helps protect them from ongoing or long-term damages from a crime that could threaten their organization and ultimately, the future of their students. Forward Edge recognized this and the needs of their customers and would look to the next steps, but this would require time and effort, and so began the drive to build a task force to solve this problem.

The Task Force

Our task force was assembled for the sole purpose of discovering the future landscape of cybersecurity insurance initiatives and the transitions or solutions needed for schools to meet those requirements. The first known initiative was to implement MFA to better secure resources. In short, MFA is the process in which a person would be required to provide more than 1 form of verification to gain access to a resource, like logging into a computer. But we couldn't just stop at MFA; we would also need to determine the best methods or standardization of any solution(s) that would allow for any future developments and initiatives of cybersecurity insurance requirements as the insurance policy landscape evolves in the future.

> Our task force was assembled for the sole purpose of discovering the future landscape of cybersecurity insurance initiatives and the transitions or solutions needed for schools to meet those requirements.

The Brains Behind the Operation

CYBERSECURITY

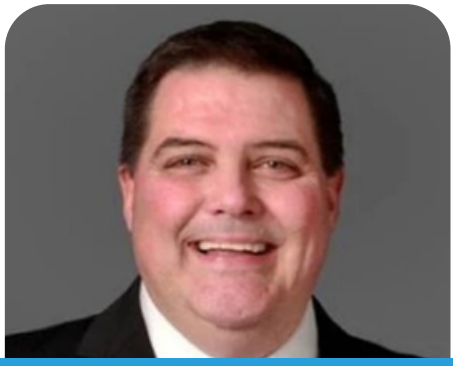
Forward Edge has put together a team of highly skilled leaders who are experts in what they do. Spanning from a variety of different departments and experience levels in K-12 education, this team is designed to provide first class consulting that fits your needs.

John Waltz
CEO

William Cirone
CIO

Chris Infante
Engineering Director

Denise Caccavari
Cybersecurity



Larry Parece
Technology Director

Kehlan Rutan
Cyber Engineer

Dustin Bingham
R&D

Devan Morrison
Remote Manager

Meet the Team

We knew that we needed a diverse team of experts in many different fields to best plan and look for solutions that could support any customer. We needed strong knowledge in multiple fields and skillsets to better dive into the task and work together to determine our best course of action.

John Waltz - *Chief Executive Officer and Founder of Forward Edge*. John is highly experienced in understanding customer needs and building solutions that meet those needs from the ground up and has always had the service mindset at the core of his being.

Christopher Infante - *Director of Engineering.* Chris knows that at the heart of any successful organization, specifically infrastructure, a healthy and thriving network is critical, and protecting the stability of that system is paramount.

William Cirone - *Chief Information Officer.* William brings years of experience to the fray, specifically in Information systems and Management, much like Chris, William understands that like the systems of the human body, a technology infrastructure must be treated and maintained just the same.

Larry Parece - *Director of Technology for West Clermont School District.* Larry lives and breathes the school environment every day and works diligently to ensure every student and staff member has the best possible experience with technology and brings an important perspective to the task force.

Denise Caccavari - *Director of Cybersecurity.* Since Day 1 of joining the Forward Edge family, Denise has made it her mission to learn all things Cybersecurity in and out, not only in policy or solution but also to include Insurance and legal requirements. Denise is a core member of the task force and brings a wealth of knowledge to our team.

Kehlan Rutan - *Security Engineer.* Kehlan began in day-to-day tech support in the classroom and over the years worked his way up to a District Technology Coordinator and has now become a Security Engineer. His experience in the classroom, management of technology, and knowledge of security made him ideal for the task force.

Devan Morrison - *Remote Management.* Devan, much like the others, has a whole slew of experiences. His details-driven personality ensures he pays close attention to even the minute details. Because of this nature, he was an easy choice to bring into the task force.

Dustin Bingham - *Special Projects.* Dustin brings an open mind and logistics-based experience to the task force. His past roles in managing technology teams and his time in Nuclear Security for the USAF would add unique expertise that works well with the other team members. His analytical and logistical skills made him a sure fit for the team.

Simplifying Your Security with MFA

There are many different MFA solutions available, so we wanted to make sure that whatever solution we selected, we would need to fully support and understand that solution to better serve our customers. The solution would also need to be able to meet the MFA requirements of as many different insurance policies as possible without compromising our core goal. We believed it would be best to avoid any service that would require the implementation of multiple solutions and over saturating the customer with unnecessary products just to check a box on a list. We needed to find a solution that could meet any possible future requirements, not just the current requirements, as we fully believe that insurance policies will continually change over time. We determined that we needed to look for a more future-proof solution to limit the burden on the customer and ensure protection for the long term.

We wanted to look at not only the support of MFA, but also **Single-Sign-On (SSO)**, **Password Management**, and even **mobile application or hard token support**. In our research and testing of solutions, we quickly noticed how truly different solutions were, some supported *ONLY* password management, some MFA only, and some only a combination of 1 or 2 of the many different aspects we'd be interested in providing to better meet future changes. We would need to test many different solutions. These solutions would also need to support the entire infrastructure as a whole, not just end-user interfaces.

Helping Districts Stay Vigilant

Due to the nature of the underfunded technology and security infrastructure of schools, they are typically slow to react in adapting to new threats and changes. Insurance has chosen to take a new methodology to better help customers remain vigilant in their security. Through changes in requirements, Insurance organizations are creating a shift in culture for many schools to set a better and more mutual standard to protect one another. For example, an organization that fails or disregards minimal or even moderate security measures opens their entire infrastructure up to cybercrime and by doing so not only makes themselves liable but their insurance organization liable; if a customer doesn't assist in taking the proper precautions to protect themselves, how long can an insurance policy protect them? So with changes in requirements and driving a shift in cybersecurity awareness, Insurance organizations are helping schools through mutual developments.

As a first step, Forward Edge began to reach out to Insurance companies and schools to learn of upcoming Insurance changes to cybersecurity policies and what schools would need to do to remain insured in the event of cybercrime. One of the initial changes would be the implementation of Multi-Factor Authentication (MFA) protocols, to better protect their infrastructure and end-users against threats. MFA is a series of processes in which a person must provide two or more verification factors to prove their identity to gain access to different resources. An implementation of MFA would certainly be a significant change that could more thoroughly protect any organization from cybercrime and be a little easier to implement as a first measure for any type of organization. This would also require specific systems and items within a school's infrastructure to have MFA enabled to meet their insurance requirements.

During one of our first initial conversations, the task force asked many different questions, some including:

- **Geo-based Authentication?** Could security be implemented that could allow access based solely on their geographic location?
- **Have Insurance Organizations or Schools worked with Unions** in the past in helping to determine a mutually agreed upon direction for security initiatives?
- **What about student authentication?** At some point could requirements change to require students to also implement security for all of their school devices?

Applying What We Know

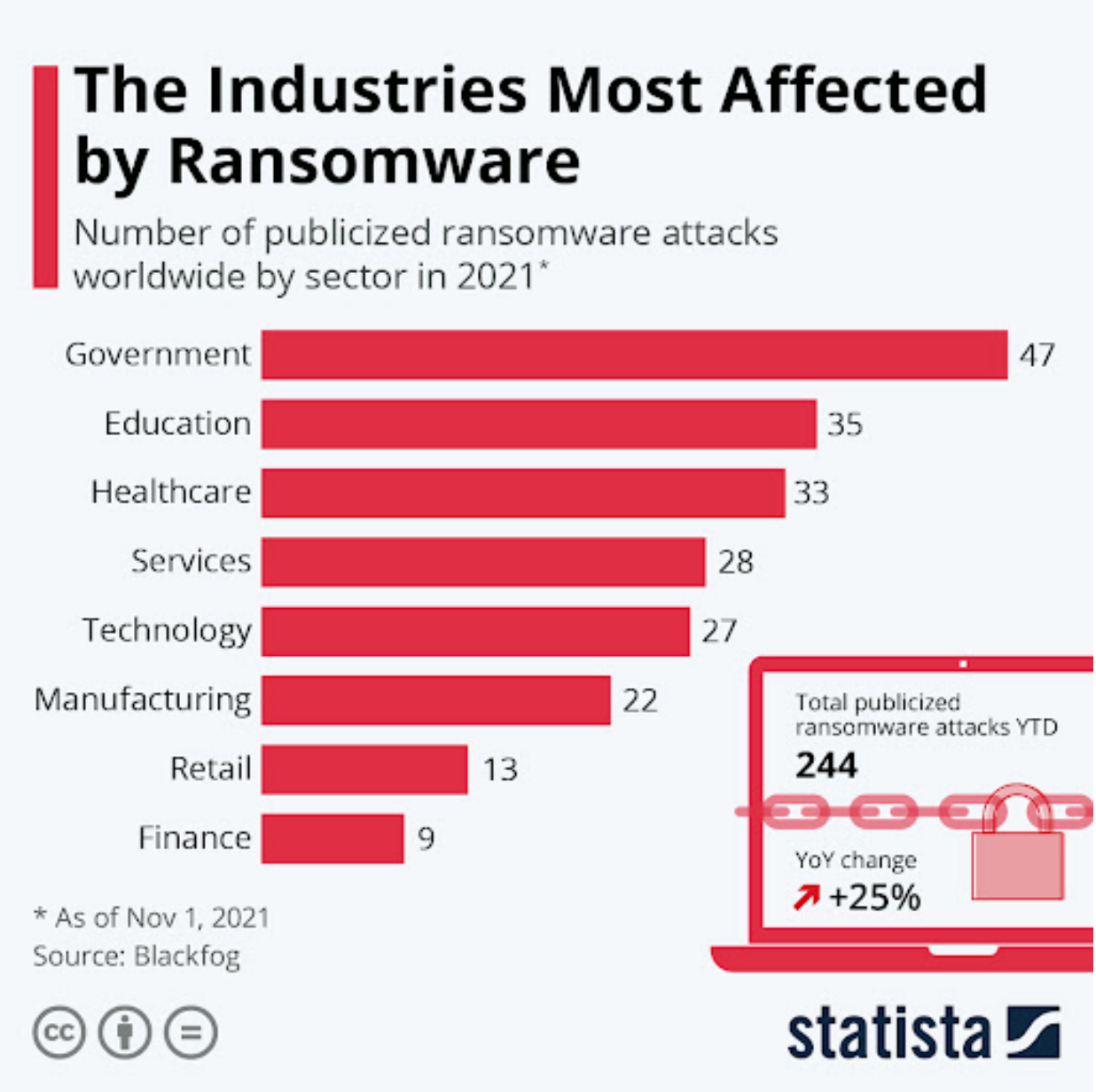
Many topics and discussion points throughout our task force's work were presented and documented as a part of our process. These data points would help us in determining the direction and assist in navigating our conversations with schools and insurance providers. One of the biggest topics of discussion revolved around the future solutions themselves. A few topics of debate:

- **What level of complexity would be required for schools and how do we determine priorities when implementing solutions?**
- **What factors are convenient and what is most easily standardized for schools?**
- **How many solutions are there and which ones are most compatible with schools?**

Most solutions are geared toward business and enterprise systems, with support for K-12 organizations typically lacking. Understandably, the differences between business and education industries are too many to count. So when comparing the two against what solutions can work and remain within affordability, we had a tough challenge ahead of us. We had to work hand in hand with different solutions providers to test and work out the best possible product for our education customers.

Attacks on Education: K-12 in the Crosshairs

It was clear from the graphic and linked articles below that cyberattacks on K-12 school districts quickly catapulted this market segment into the unenviable position of being among the most targeted in the world. A rapid increase in technology adoption due to the COVID-19 pandemic, coupled with already meager cybersecurity funding, made the K-12 market a hunting ground for cyberattackers. Of course, these factors have not escaped the notice of cyber insurance underwriters.



Cyber Attacks Record-Breaking Year
Cyber Actors Targeting K-12
Schools Have Become the Leading Targets of Ransomware Attacks

WCSD Tackles MFA

When it came time for West Clermont Local School District (WCSD) to renew its cyber insurance policy in the late summer of 2021, the application looked very different from previous years. Many questions remained from earlier versions:

- "Does the organization maintain data backups?"
- "What is the frequency (daily, weekly, monthly, etc)?"
- "Does the organization use antivirus software on end-user devices?"

A host of questions asked if **Multi-Factor Authentication (MFA)** was required when authenticating to different systems and devices throughout the organization, even some hosted externally.

- Server administrator accounts
- Management connections to network components
- Virtual Private Network (VPN) connections
- Backup manager credentials
- Accounts with elevated access on user workstations

All of these areas were called out specifically in this new age application. While we've always known these systems needed to be at the center of our security focus, it was very clear that insurance carriers were now hyper-aware as well.

Responding to these questions kicked off discussions at WCSD around how many of these protections were in place, how many were planned on the current roadmap, and what would be required, both in time and treasure, to implement these more quickly and adopt the rest. The sheer number of references to MFA in the insurance application placed it at the top of the list for conversation. MFA was already on the district's cybersecurity roadmap, but implementation was still a year off. The question was, "Could these be set up in a week? Two? A month?" The answers were, "No. No. and Possibly..."

Cloud-based Email Service (Google Suite)

Having merged its Microsoft Exchange email into its Google GMail domain a few years earlier, WCSD was standardized on the Google Workspace environment. Turning on MFA for the entire Google Suite was a matter of a few clicks. Introducing changes to the way users access those tools, however, would be a far more time-consuming proposition. An organization-wide announcement, followed by a litany of messages, prompts, and reminders would be necessary before a change of this magnitude could be enforced. Too, though MFA can be enabled in moments, equipping staff members to successfully navigate registration and use of USB Keys and/or Authenticator Apps (i.e. Microsoft or Google Authenticator) would require a great deal of time and coordination.

Identifying the Right Solution

So which tools are needed to activate MFA to the degree that many cyber insurance carriers currently require? Well, that depends. There are many options available from a variety of manufacturers and software publishers, and they take several forms. WCSD investigated software-based solutions like Microsoft/Google Authenticators and Authy, text messaging, and Google prompt. Hardware keys like Duo and Yubikey were also considered.

- **Authenticator apps** were an attractive, low-cost solution as virtually every user has a personal device that can be registered to their account and receive prompts when logging in, however, some users objected to using their device for work purposes.
- **Text messaging** as a form of MFA was considered for its simplicity, but it was ultimately excluded because text messages are sent in "plain text", unencrypted, making them prone to interception.
- **Hardware keys** presented an attractive, standardized solution for those users who objected to using a personal device to facilitate their work. The drawback is that these are fairly expensive.

When making a selection(s) of one or more methods for accomplishing MFA, it is extremely important to inventory every system *AND HOSTED SERVICE* that houses sensitive information or could cause significant disruption to the organization if compromised. The list should include all on-premise servers (Operating Systems), hosted solutions, infrastructure components (switches, firewalls, wifi, etc.), virtual private network or remote desktop access, etc. Once a comprehensive list of systems in need of MFA security has been crafted, it is then possible to identify which of the available solutions are capable of providing second-factor authentication to the greatest number of those. You may find no single solution capable of securing them all. A traditional Venn Diagram will quickly show the most versatile choices and assist in creating a comprehensive plan.

WCSD investigated multiple strategies/products to enable MFA across the district's sensitive systems and infrastructure. As an organization familiar with the Fortinet Operating System (FortiOS), weeks were invested in working with Fortinet specialists trying to implement the FortiAuthenticator appliance. Ultimately, it was learned that a comprehensive migration from on-premise Active Directory (AD) to Azure AD would be necessary to make this solution viable. Too, to use the FortiAuthenticator, it is best to deploy FortiTokens as the USB Key of choice, something WCSD was not prepared to do.

3 Key Phases for Implementing MFA:

Discovery

Determine Requirements

Process

Prioritize Discoveries & Implement Processes

Review

Audit Discovery & Implementation Phases

Pursuing an option for MFA security on Windows accounts housed in on-premise AD led the district to GreenRadius, an MFA proxy solution by GreenRocket. Others are likely to exist, but this product came highly recommended, and time was running short. Using GreenRadius, WCSD could secure the full collection of systems and services on its list. Users were allowed to choose one of two methods to achieve MFA, an app on their device or a USB key (text messages were excluded from the outset for reasons stated above). App users were given the choice of using Microsoft Authenticator, Google Authenticator, or Google Prompt on their devices, and all others would be issued a USB key. To ensure the USB keys would serve current and future needs, options were evaluated for compatibility with the list of sites and services requiring MFA, and, for various reasons, two made the shortlist, **Duo and Yubikey**. Both are compatible with Google Workspace and Microsoft 365 and meet the requirements for MFA of "cloud-based email accounts" specified on cyber insurance applications. Digging into each product revealed that either seemed to meet the needs of a more comprehensive MFA implementation by securing network infrastructure and remote access credentials. Ultimately, WCSD opted for Yubikey and its "one-time cost" rather than the subscription-based model offered by Duo.

Selecting the key manufacturer was the first step, but Yubico makes a couple of flavors of USB keys. The more capable the key, the more costly, so while future-proofing the solution by selecting a key that meets a user's need both now and, at the very least, for the next few years was of paramount importance, it was necessary to consider each stakeholder group and the accounts used by each. This preparation was important to avoid buying expensive USB keys when those at half the price would work well for most users. In the end, it was determined that users with escalated administrator privileges (the I.T. Team), users requiring remote access (about 7%), and infrastructure managers were the only groups needing higher-end keys capable of MFA in these specialized cases. Most users (90%) would be served well by a basic USB hardware key at half the price. These users, needing only to secure their Google Workspace account (and eventually their Windows user account when that mandate comes), were issued the Security Key Yubico (SKY) key. The limited number of users requiring MFA on a broader range of systems and services (Remote access through VPN, Elevated Windows Administrator Accounts, Switch, Server, & Firewall Managers) were issued the Yubico Series 5 key. Supporting several additional protocols, it proved to be the right choice for this limited group of users.

Our Method in the Making

During our testing, we couldn't just demo, play around, and give it a thumbs up or down. We needed to be more sophisticated in our direction, workflow, and methodology. We needed to develop a method of documentation and a knowledge base to properly compare and contrast each option so we could choose the best possible solution and support thereof.

We built out a grading matrix that could sufficiently log and track each solution as we worked through them and kept a record of what kind of overall score we gave the solution. To do so, we all worked together to determine categories of importance so we could apply a binary grade of 1 or 0 in each category for each solution. From there, we added weight factors for each category based on our determined level of priority of those categories. For example, Cost is always a concern for any customer, so we placed a higher weight on grades earned by a solution that featured acceptable costs for a school. If a solution was better than expected in a category it would receive a 1. In cases where the solution was simply acceptable or as expected, **it would receive a grade of 0**. In cases of a solution having less than ideal features or supports in any given category, **it would receive a -1.**

Categories	Compatibility	Customer Costs	Complexity	Ease of Use
Product #1	-1	1	1	0
Product #2	1	1	0	-1
Product #3	0	0	1	1

For several months, we spent time designating and redefining our categories and settling into areas that we felt would matter the most to our customers. We took those categories and defined them through a rubric and applied it to every solution. We generated a document that defined each category and whether or not each solution satisfied insurance needs, customer needs, and of course, whether or not a solution was compatible with those needs overall. We documented each aspect of every solution and made sure to apply our defined categories against them. As an additional measure, we also considered the long-term use of the solutions overall so we could determine the perceived length of time the solution could satisfy insurance requirements without significantly changing solutions or impacting customer security practices year after year.

Step by Step Solutions

We then needed to consider the proper process to implement the solution or any solution for that matter. Not to mention, we also had to consider the transition of any new implementation as we needed to be sure to care for and provide guidance to our customers while simultaneously managing the process and quality of the solution.

We began by considering all of our past transitionary projects and services. We poured over our historical processes and experiences to better understand the good, bad, and ugly of any new implementation and we deep-dived into all the steps we followed throughout our experiences. Unlike before, this would be an entirely new process as we had to consider covering all the requirements of customer insurance policies, which would modify our previous plan of integration. For example, our engineers could easily generate a list of how to properly secure servers, switches, or other systems, but Insurance and our customers may have an entirely different perspective on what is a priority. What about an organization's student records, shouldn't they have the highest priority? Or how about email traffic and communication?

So as our next step, we scrutinized our past practices and realized we couldn't follow our normal methodology. Through a long strenuous task of laying out our past practices and aligning them with the customer and insurance policies, we worked out the best possible process to meet all requirements while still meeting best practice standards developed over the lifetime of our services.

From that moment, we began to document our new process and generate the necessary white pages and workbook policies to best implement an MFA solution worthy of satisfying insurance requirements, and maintaining customer security and satisfaction. Our process follows three distinct phases; **Discovery, Implementation, and Review.** Through this process we can ensure quality work, we follow a high standard of methodology, and we remain transparent and collaborative with our customers and any other parties involved with their security transition and implementation.

Design **Implementation** **Review**

Three Stage Success Strategy

Discovery is the portion of our process in which we work with the customer to determine each aspect of the requirements and understand what they currently have in place and what areas of concern we would need to address to secure their organization, so in this way, we can build a high-level view of the project and know the playing field.

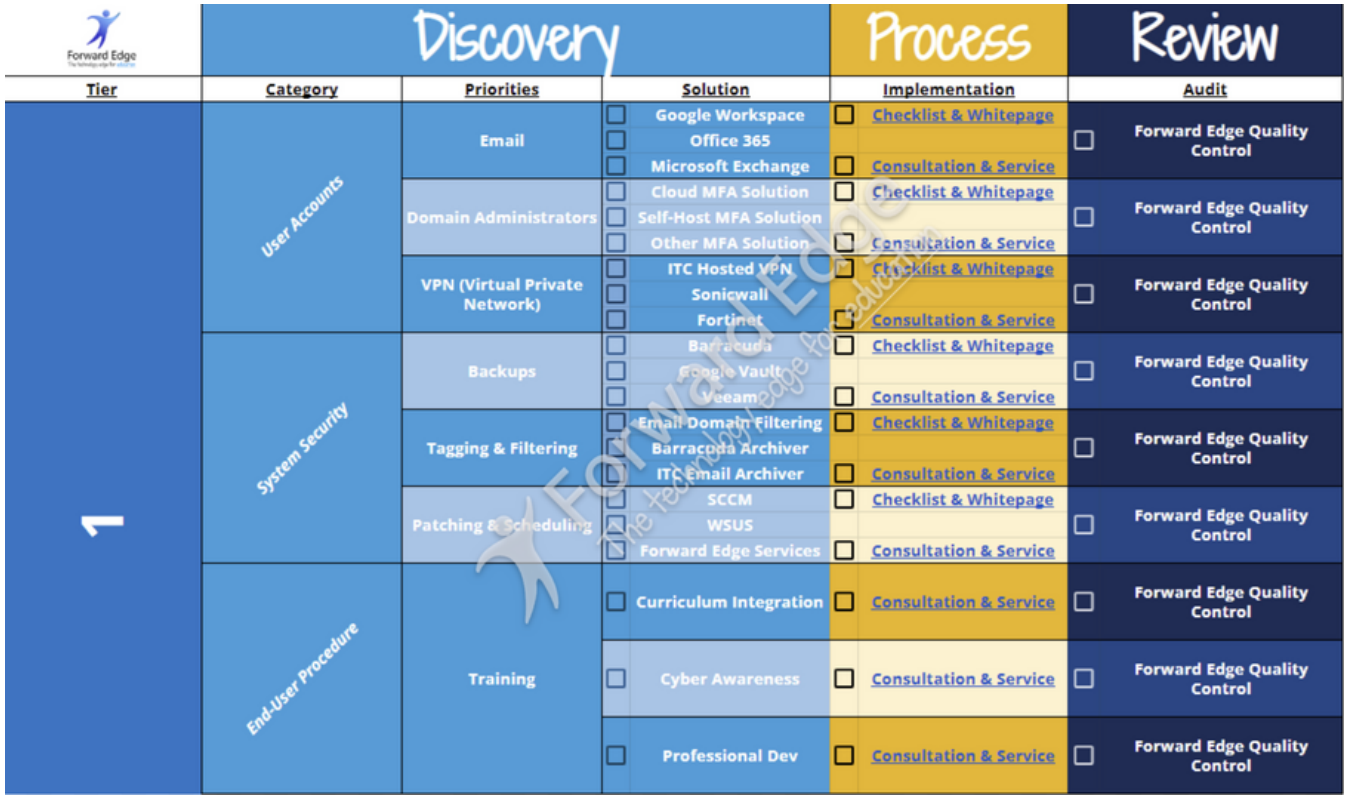
Process is the portion of our approach in which the real integration and work would be completed. In a simple sense, we start from the highest priority items in the organization and work our way through all discoveries and implement these processes. But the involved portion of this work is that for each requirement and priority we have generated all necessary white pages and checklists for our solutions and services as well as the white pages of any third-party solutions or services that will also require attention during this stage.

Review is the final portion of our process in which we will audit both the Discovery and Implementation phase to ensure that we have met all requirements, and have analyzed and evaluated all implementations so that we can ensure we did not skip any portion of our process and to account for anything we may have overlooked. It is then within this final phase of our workflow that we work back through and verify everything with our team as well as the customer. This way we can generate feedback, discover hiccups, and re-engage as needed. And last but not least, this final phase is the portion in which we review our entire project with the customer to ensure that our solution is fully implemented and operational.

> It is then within this final phase of our workflow that we work back through and verify everything with our team as well as the customer.

Laying It All Out: A Deep Dive into Our Process

Previously, we mentioned that through our process we generated a **three-phase system** and workbook to help manage and control our process overall. To elaborate, this workbook and process involve a multitude of policies and white pages to help manage all of the different aspects of implementation and controls necessary to succeed. On top of these, we also developed a proper checklist for each priority and aspect of concern when implementing our solution.



Forward Edge	Discovery			Process	Review
Tier	Category	Priorities	Solution	Implementation	Audit
1	User Accounts	Email	Google Workspace Office 365 Microsoft Exchange	Checklist & Whitepage Consultation & Service	Forward Edge Quality Control
		Domain Administrators	Cloud MFA Solution Self-Host MFA Solution Other MFA Solution	Checklist & Whitepage Consultation & Service	Forward Edge Quality Control
		VPN (Virtual Private Network)	ITC Hosted VPN Sonicwall Fortinet	Checklist & Whitepage Consultation & Service	Forward Edge Quality Control
	System Security	Backups	Barracuda Google Vault Veeam	Checklist & Whitepage Consultation & Service	Forward Edge Quality Control
		Tagging & Filtering	Email Domain Filtering Barracuda Archiver ITC Email Archiver	Checklist & Whitepage Consultation & Service	Forward Edge Quality Control
		Patching & Scheduling	SCCM WSUS Forward Edge Services	Checklist & Whitepage Consultation & Service	Forward Edge Quality Control
	End-User Procedure	Training	Curriculum Integration	Consultation & Service	Forward Edge Quality Control
			Cyber Awareness	Consultation & Service	Forward Edge Quality Control
			Professional Dev	Consultation & Service	Forward Edge Quality Control

Our checklists and white pages follow an open-ended process that not only allows us to do our work but could be followed by customers who wanted to play a more active role in their solution implementation. This allows us or the customer to follow a line-by-line style process to help manage implementation step by step. If customers wish to use their team for implementation, they would be able to fully follow our process and implement security solutions on their own. In these cases, rather than act simply as a service provider and manage the transition on behalf of the customer, we could also act only in a consultative manner and provide a more guided approach for our customers and engage only as needed per the customer's wishes.

We felt that in this way, rather than keep things out of reach for our customers, we'd remain **transparent and collaborative** in the process. We also wanted to be able to provide a clean process that anyone could use as guidance during what is already a complicated process that dynamically changes an organization's posture and approach to a successful security practice. We made sure that our checklist covered even ambiguous processes or work that would inevitably be involved, such as the discussion and shift around cultural change within an organization. For example, how will MFA affect day-to-day operations for staff and the organization overall and how will the administration communicate their transition?

Tested, Tried and True

We generated alpha tests with many different solutions and through many different participants. As we got closer to grading and finding our better-matched solutions, we would move to beta tests with other participants. We would document all feedback and document what went wrong, what went right, and any negative or positive feedback gained from our participants. Over time, we were able to fully test our grading matrix against several of the top choice solutions. From there, we fully tested our workflow process against those solutions. We didn't move as quickly as we had anticipated and ran into hiccups. From one solution not being compatible with anything other than proprietary hardware or software, to solutions that were so compatible that it was a security flaw.

And after many months of trial and error, we finally discovered what we believe to be the best possible solution that could satisfy insurance requirements, increase security posture, and provide the most return on investment to our customers. For the solution to be successful AND satisfy the needs of our customers though, we felt that we had to make sure it was **absolutely** right and what better way to ensure success than to implement the same solution within our organization. We stand by our services and our work, so we wanted to put the solution to the test even against ourselves. Through trial and error, internal training, and small changes day by day, we were able to fully implement and test the solution within our infrastructure and teams.

For the solution to be successful **AND** satisfy the needs of our customers though, we felt that we had to make sure it was **absolutely** right and what better way to ensure success than to implement the same solution within our organization.

Our Guarantee to You

As we come out of the pandemic, cybercrime isn't going to relent. Cyber threats will only continue to escalate and threat actors will continue to look for new ways to put a strain on organizations around the world. And based on current trends, the education industry will continue to see a rise in cybercrime, and ultimately significant effects on cybersecurity policy as it forces inevitable changes in posture over the next few years.

As covered, one of those changes lies in the world of Multifactor Authentication and how we can help schools overcome the ongoing changes with policy and their insurance over time. Through our deliberation over the last year, we feel that we've spent a significant amount of time to better account for what is most important and what takes priority for any customer to best match the possible needs of schools and simultaneously satisfy the needs of their insurance providers. Through grading different solutions and options into an analysis matrix, then testing those various solutions in-depth to compare their various features and compatibility with different environments, we were able to lock on to the most fitting solutions for a majority of insurance as well as school's needs.

Through our task force and the combination of everyone's expertise, including our partnership with WCSD, we were able to lock in what can help ensure a stable path for the future of cybersecurity and insurance needs for schools and our customers.

CYBERSECURITY