ARG
IT Clarity®

CYBERSECURITY

Market Insights & Decision Guide

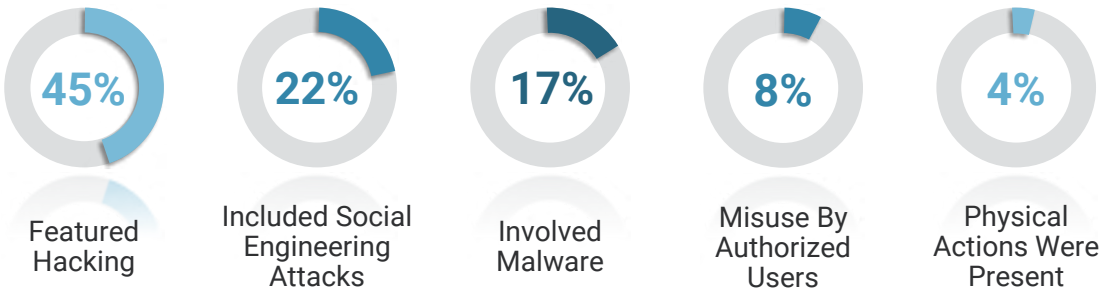
What Happens to a Threat in a Virtual World?

Business technology has changed drastically in the last five years, and 2020 saw a complete reshaping of the technology delivery model. Years of change were compressed into a few months. Computing is largely accomplished in the cloud, and what is not in the cloud will likely move to the cloud in the next server refresh cycle.

Major business systems have been outsourced to third-party software providers. Workers need to access these resources from anywhere on a variety of devices. Work from home is now the norm. In addition to how we access resources, and from where, the cyber threat landscape has become much more complex. Cybercrime is now a mature and significant business in many parts of the world. Sophisticated operators, some backed by nation-states, are working diligently to compromise your systems.

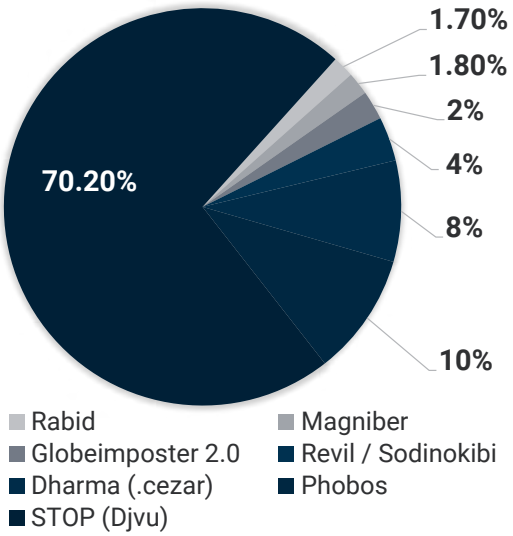
The first half of 2020 saw the line between a ransomware attack and a data breach continue to blur. Much like Maze, several prolific ransomware operators, including Sodinokibi, created websites where they publish the stolen data of non-paying victims.

How are the Bad Guys Getting in?



86%
of breaches were **financially motivated.**

Most Reported Ransomware Strains



Attack Vectors

Phishing - 90% of all Ransomware infections are delivered through email.

Cryptoworms - a form of ransomware moves laterally throughout the network to infect all other computers for maximum reach and impact.

Polymorphic malware - makes small changes to its signature for each payload dropped on machine–effectively making it a brand-new, never-before-seen file. Its ability to morph allows it to evade many virus detection methodologies. Today, nearly all ransomware is polymorphic.

Ransomware as a Service (RaaS) - Ransomware "starter kit" available to novice hackers on the dark web.

Targeted attacks - carried out by using tools to automatically scan the internet for weak IT systems. Targeted attacks often work by attacking computers with open RDP ports.

The Pandemic Effect

Almost 1,000% increase in phishing attempts. (Barracuda)

There are over 667 million malware programs currently in circulation. (Statista)

There has been a 400% increase in brute force attacks. (ZDNet)

Users are 3x more likely to click on pandemic phishing scams. (Verizon)

Ransomware attacks are up more than 100% from last year. (SonicWall)

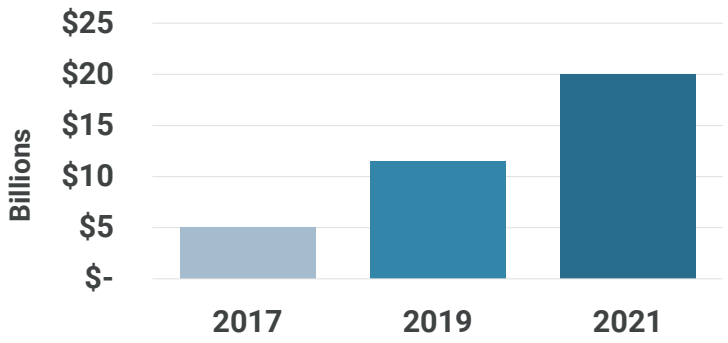
Costs Are Escalating

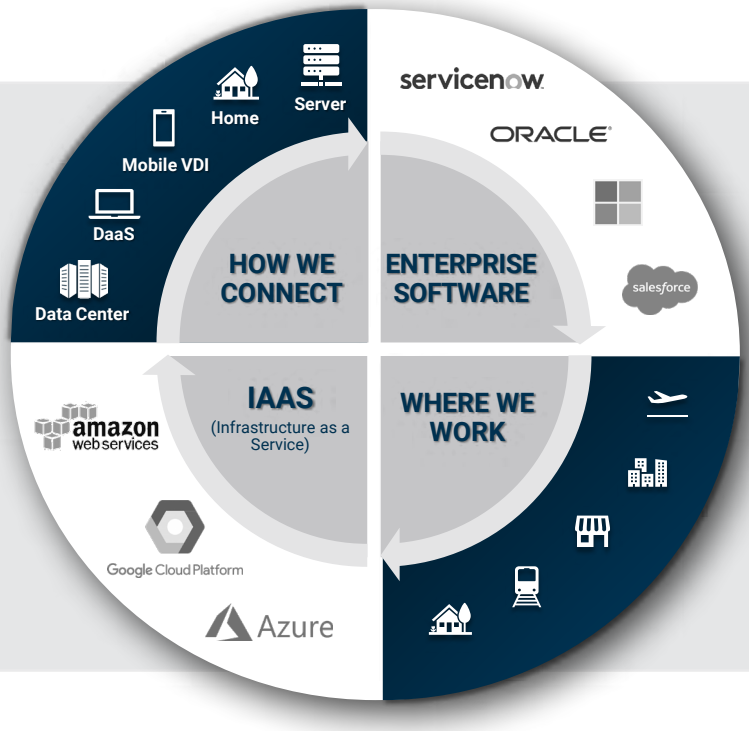
US government agencies, healthcare providers, and educational institutions were impacted by ransom attacks at a **cost of over $7.5 billion** in 2019. (Emsisoft)

70% of organizations are **increasing security spending** as a result of COVID-19. (LearnBonds)

68% of U.S. businesses have not purchased any form of cyber liability or data-breach coverage. (Cisco)

Estimated Global Ransomware Damage Costs
(Cybersecurity Ventures)





Protecting the New Edge

Today, our data centers are a fraction of their former footprint. Servers have been moved to more effective and efficient cloud environments.

Given the significant movement of assets and resources, security solutions have remained relatively static.

- Firewall
- End-point protection
- VPN

Forcing users back to the data center for security increases costs and lowers employee productivity.

Focus on Three Goals

LAYERED APPROACH

01

Deploy multiple controls for maximum protection.

PROTECTING YOUR DATA

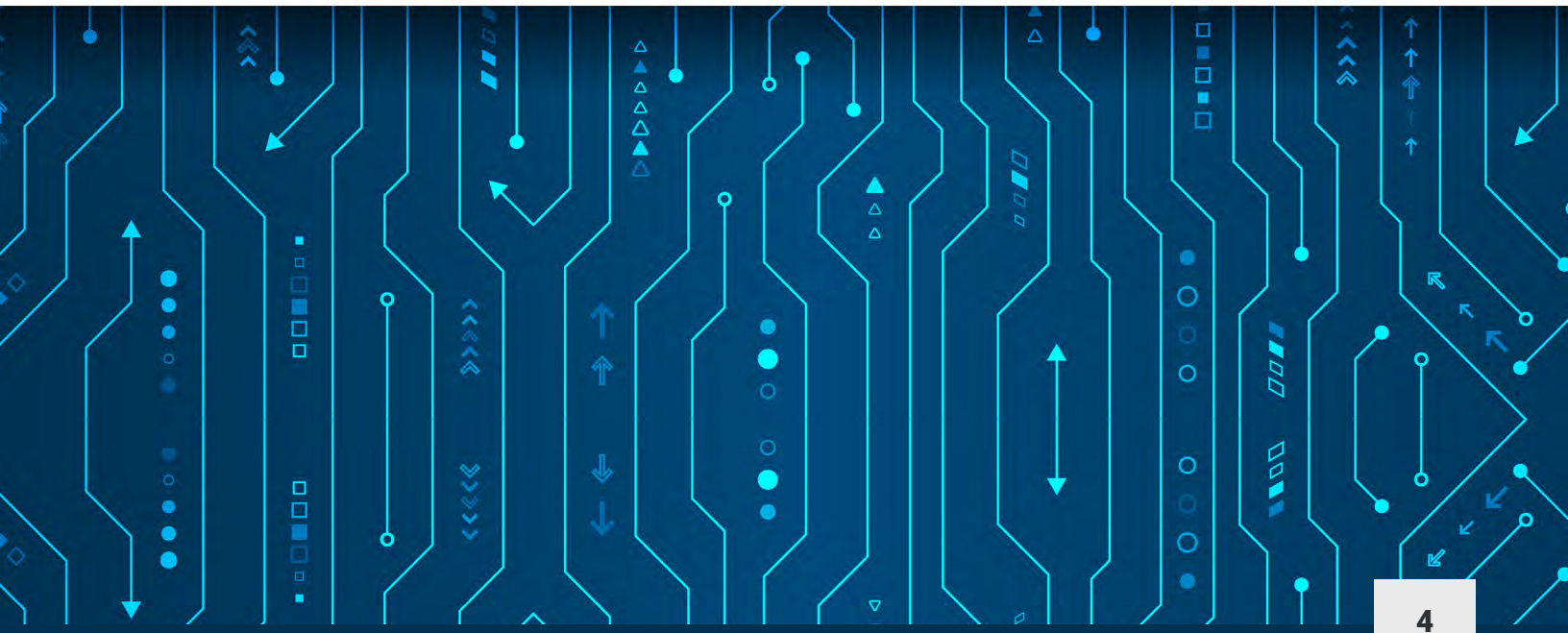
02

If you can't describe how you are protecting your data, you probably aren't.

SECURITY ELEVATOR PITCH

03

Does the auditor stay 5 minutes or 5 weeks?



Watch a Cyber Attack Unfold

Day 1

Users report issues with file access. Network monitoring platform alerts to suspicious access to the domain controller and file writing activity. Both a private cloud environment and an Azure environment had been compromised. IT decides to pull the plug on both. Emails went out to staff and triage begins with the cloud provider.

8:00 AM

Attack Detected
Files entitled "RecoveryInstructions.docx" are found in multiple folders throughout environment. The ransom note requires contact and payment in 72 hours, or the ransom escalates. The client asks their cloud provider to begin forensics and reaches out to their cybersecurity insurance provider. The client utilizes Desktop as a Service (DaaS), so limiting network access is relatively easy. Staff is told not to access the Microsoft O365 assets via the internet. Users await an update from IT.

10:00 AM

Client Responds
IT locks down environment and kicks users off desktops. Email to staff not to access desktop or shared drive. All staff call to brief team on ransomware attack. Users are instructed that Mail and Salesforce use outside of DaaS is fine, but they cannot access MS Teams or the File Server.

Initial triage shows extensive corruption in the private cloud environment, but only limited impact in Microsoft. The last private cloud backup was run the previous evening through an offsite recovery service. The service includes a full cloud-based rebuild and 30-day use. That restoration action plan is activated with the vendor. By sheer luck, a snapshot had also been taken by the private cloud service provider at midnight due to a maintenance. The shortest path to recovery is to have them rebuild the servers and reinstall the snapshot if it's clean. This recovery plan is initiated.

Insurance company advises client to speak to law firm specializing in cyber attacks and provides recommendation.

12:00 PM

Identify that SharePoint files are corrupt and shut down all apps in O365 to prevent sharing.

Receive statement of work (SOW) from law firm, approves it, and sends to insurance company for their approval.

Recovery Begins
DaaS provider restores all servers from midnight snapshot.

2:00 PM

Insurance approved SOW and Law Firm begins work. Insurance recommends forensics IT firm.

4:00 PM

Forensics firm produces SOW, and it is approved. Forensics recommends a negotiator.

DaaS provider shares that they found the open port that hackers used for access and shut it down.

Negotiator's SOW is approved by insurance. Negotiator counsels not to contact hacker as prices start escalating once they are contacted.

6:00 PM

DaaS provider confirms that 12:00 AM snapshot is not corrupted and begins rebuilding desktops with that backup.

Call with lawyer to review what steps had been taken, next steps going forward, and to confirm forensics contacts.

All users restored. IT rolls out playbook for users to follow to reinitiate their services, starting with changing passwords. An open web conference is conducted throughout the morning to provide end-user support. It has been 24 hours and the business is functioning close to normal. Forensics continues and identifies the ransomware locker used, providing insight into which hacker group is likely responsible and automatically decreasing the likelihood that data was stolen.

Day 2

Contacted hacker, the client is fully recovered. The hacker quickly proves they can decrypt but is unable to produce specific files to prove data theft. A loss of data could be devastating. Each state has different notification requirements and there are federal and FCC requirements in addition to any contractual and NDA requirements that would impact the client. Since the hacker is unable to verify data theft, the negotiator assures the client that they are in the clear. The client moves forward to complete a post incident review and identify areas of improvement.

Day 3

Additional Protection Deployed
Restored OneDrive files. Sent AV logs for corrupt servers to forensics firm for further research. Cleaned up distros and active directory. Installed CarbonBlack to identify remnants and identify any residual traces of the hackers.

Day 4-10

01 LAYERED APPROACH

What worked?

Protecting your business from cyber attacks is more than security applications and tools, it encompasses the way you deploy and configure your technology and leverage diverse platforms for business continuity. The client's business was impacted for less than 24 hours. No data was stolen, and the client only paid $10k cyber insurance deductible. Because the client used Mimecast - a cloud-based email, anti-spam, and archive filtering service - and mail through 3rd party provider, they were still able to conduct business. They also benefitted from a cloud first strategy as their SaaS applications such as voice/collaboration and Salesforce were fully available allowing them to continue to respond to customers and access the data that is critical to run their business.

Here's what the client credits with allowing them to be fully functional in 24 hours:

- Users were trained to notify the help desk.
- Microsoft alerting system was configured. Alerts helped identify where the issues were happening.
- Their DaaS solution provided full control to shut down at the admin level and rebuild.
- Third party off site incremental back up twice a day and daily automatic snapshot of environment had them covered.
- Cyber insurance with a premiere firm provided immediate access to resources to do forensics, mitigate damage, and negotiate with the hackers.
- Disparate locations of resources.
- Diverse unified communication and collaboration platforms.
- Ability to remotely control end users' machines.
- Competent MSP with multiple resources available to dedicate.
- Internal team with a breadth of IT knowledge that approached from multiple angles guided MSP response.

What could have been better?

PEOPLE

End-user training

Shadow IT – there were several users with extensive file storage in SharePoint. End users replaced the corporate standard of saving files on the fileserver for the ease of SharePoint. Microsoft has some native back up, but not a full DR. Securing and backing up Microsoft, Box, or whatever platform your users are leveraging will minimize disruption.

PROCESS

Regular pen tests or vulnerability scans would have caught the open port.

Governance – Outdated active directory distros made it difficult to identify unauthorized additions. Better governance would have addressed this and is particularly important if you are using the federation capability of Teams.

TECHNOLOGY

Managed Threat Detection

Microsoft Alerts

Investment in Advanced Endpoint Protection

Advanced Threat Protection – AI / Machine Learning

Here are the most common strategies our clients use to protect their environments:

"OK"

Management of Prem-Based Servers + VPN

Pro:
Leverage third party to compliment in-house skills.

Con:
Recovery would include physically touching devices or sending users "media" (i.e. USB drive) to recover.

This could mean inserting a USB drive into each server or machine to resolve — in today's environment that could take weeks.

"BETTER"

Add improved technology, people, & processes.

This could include; Multifactor Authentication (MFA) + Cybersecurity Awareness Training + Remote Monitoring Management.

Pro:
Addresses most common attack vectors.

Con:
Lacks intrusion detection & prevention. There is still risk for online file sharing—SharePoint / OneDrive.

"BEST"

Next-Gen cybersecurity with layered technology.

This could include; DaaS + MFA/ SSO + Backups + Managed Threat Detection or XDR and CASB/DLP (Cloud Access Security Broker/Data Loss Prevention)

Pro:
Layered approach minimizes exposure and allows for the quick rebuild of user desktops remotely.

Con:
Can create complacency. Process and training still required. Balance control with user impact.

Cyber Insurance Cost & Reward

In the client example, a firm with $180M in revenue reported paying about $15k annually for a comprehensive policy with a $10k deductible. This provided:

- $1M first party expenses with $3M total aggregate limit
- Separate business continuity policy
- Crisis management if data is exfiltrated
- Regulatory responses, compliance requirements, and client communications
- Business interruption loss
- Cyber investigation and extortion expense - fees you pay to the bad guys
- Data restoration expense—if prem could mean new gear in the "data center"
- $50k for forensics, law firm, and negotiating firm
- Security insurance can include services such as;
  - Complimentary phishing service—that includes training for end users and testing
  - Cost of AntiSpam services like Mimecast or Proofpoint
  - Cost of Phishing services like KnowBe4
  - BitSight service or similar which scans and provides security rating

Where to Focus

Cybersecurity can be overwhelming! Look to focus on the following tips to improve your security posture.

What?	How?
Know what you have.	Build a usable inventory list. Use tools like Windows management, patching, endpoint protection, and spreadsheets to help identify systems, applications, cloud assets, vendors & partners who are storing, processing or handling your data.
Have a tested backup and recovery plan.	Don't forget cloud assets (M365)! Third party off site backup that is regularly tested. Backups should be air-gapped from providers — if MSP gets hit there's a strong possibility that both production and BU can be affected. Ensure MSPs are leveraging outside solution for protection.
Thoughtfully manage your identities.	Enable multi-factor protections and consider single sign on or team-based password management tools like LastPass or 1Password.
Keep current.	Regularly review accounts & disable or remove old / unused /inactive ones.
Monitor and limit access.	Zero-trust is the preferred way of limiting access. More traditional methods included network access controller and Active Directory profiles to limit access to sensitive information.
Be an informed skeptic.	Develop and trust your gut. Leverage regular training and education tools to help inform staff. (e.g. Knowbe4, Cofense, Wombat)
Security can be a team sport.	Thoughtfully deploy external help or managed services. Expanding your team can provide better monitoring and coverage options, scalability, as well as expanding your subject matter expertise.
Develop a risk management program.	Remember to communicate often, discuss realistic scenarios, and monitor resulting to-dos. Security discussions should be cross functional and not solely include IT or security.

Does the auditor stay 5 minutes or 5 weeks?

How tight is your security pitch? Can you confidently state the following?

Please rate the below on a scale of 1—5 (1 = not confident; 5 = completely confident)

- _ I know what I have. I have documented my organization's IT & Cybersecurity inventory.
- _ I am securing my identities. We require long, unique passwords augmented by MFA where possible.
- _ I limit access based on business requirements and regularly review accounts (local, Active Directory, cloud, etc.)
- _ I think before I click and am developing a healthy skepticism.
- _ I leverage enterprise class tools.
- _ I carefully leverage managed services that provide business value.
- _ I manage my cyber risks and regularly discuss scenarios with my team.

Don't Reinvent It! Use well regarded guidance from the following resources:

NIST Cybersecurity Framework (CSF)
https://www.nist.gov/cyberframework

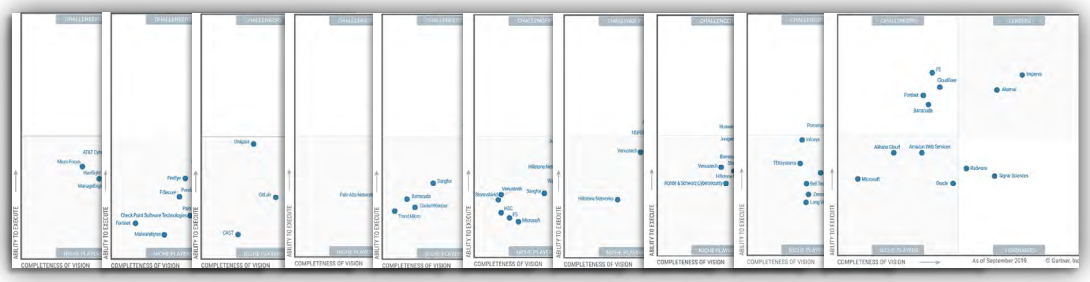
ISO 27000: Information Security Management System
https://www.iso.org/news/ref2477.html

Center for Internet Security (CIS) Top-20
https://www.cisecurity.org/controls

Cybersecurity Maturity Model Certification (CMMC)
https://www.cmmcab.org/

Fresh Perspectives Rarely Evolve from the Status Quo

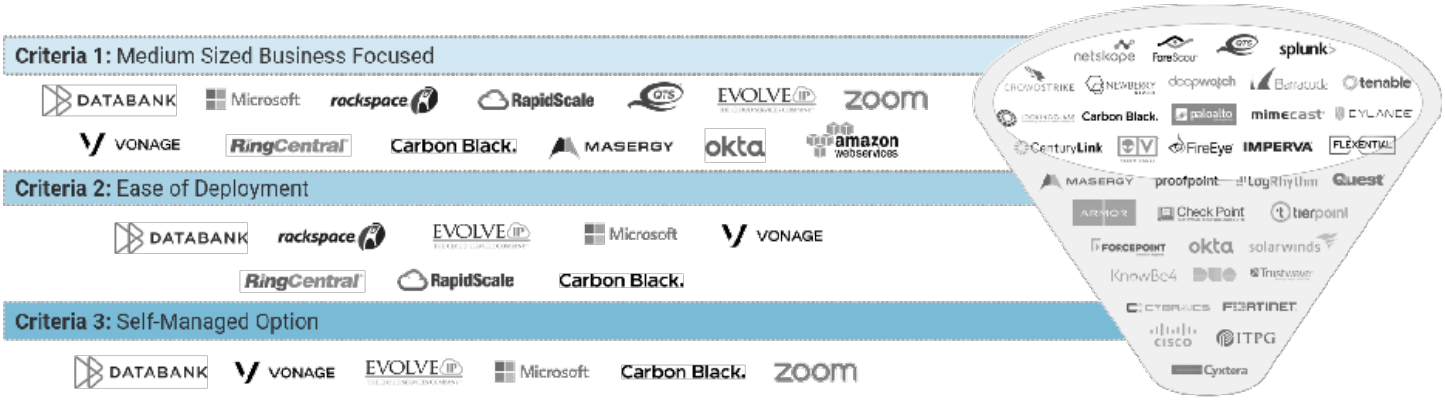
Gartner has ten Magic Quadrants related to cybersecurity and more categories that they are tracking. There are thousands of potential solutions. As leaders, we must conduct a diligent process of requirements gathering, strategizing, provider candidate selection, evaluation, negotiation and implementation. So, what's the best approach to take to achieve that?



The decisions must enable the business' mission, support a dynamic workforce and keep agility in mind for the ever-more rapidly changing landscape. Your plan should also arm you to respond to auditors and improve your security rating.

Path to the Right Decision

A deliberate approach is critical when deciding on a platform because navigating the pace of change and overwhelming choice in the market is a significant resource challenge for any IT organization. ARG identifies the right solution by following an established framework to map the desired business outcomes and current investments to the most robust integration and performance criteria displayed by service providers. We bring perspective gathered from thousands of technology implementations and post-installation service that we manage for our over 4,000 clients.

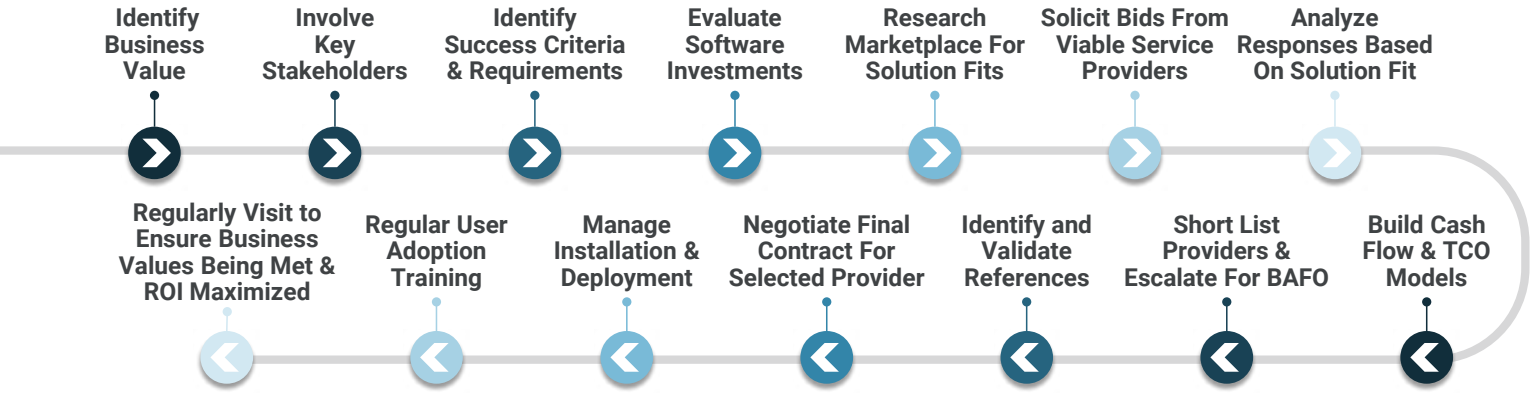


"ARG has provided us with only the best and most knowledgeable support for over 10 years. The teams they deploy to shepherd any project has ensured a seamless experience and a steady focus on the process, every time. ARG has consistently delivered its top talent to help inform our service procurement decisions. We are grateful for this partnership!"

- Deborah, Forest Trends

Understanding the solution provider's ability to execute against your most critical criteria is the difference between making the right choice and having a project that misses the larger business value. Once a solution is selected, ARG's continual monitoring of market conditions and experience pricing solutions for thousands of clients ensures the best price, and best value, by leveraging the maximum benefit from available offers and promotions.

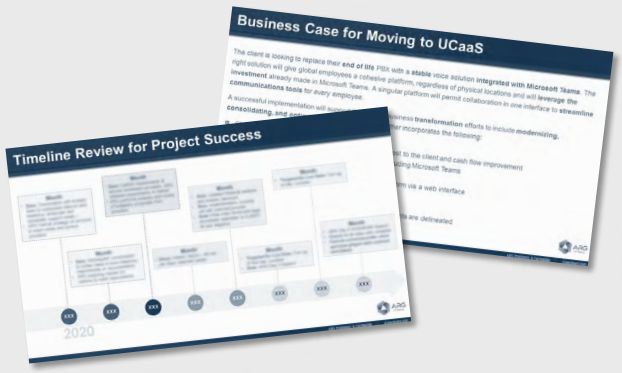
ARG's Thoughtful Decision Process



Meeting with the Board

To support the right solution for an organization, ARG helps clients prepare the presentation for their board. This presentation justifies the solution by thoroughly documenting the selection process. We prepare you to field questions from the board room, your leadership and your peers. You will be prepared to inform them with the detail they need to approve your recommendation:

- Why are we making a technology change? What are we looking to achieve & why?
- Were we inclusive? Who was involved in the decision?
- What process did we follow?
- What are our requirements & measurement for success? What business value will we achieve?
- What approaches did we consider? Roughly how much does each approach cost?
- Did we look at everyone? How did the suppliers stack up?
- Are we getting the best deal? Cash Flow? Net Savings?



There is no charge to engage ARG to evaluate the market on your behalf. Contact us at info@myarg.com to schedule a consultation.