Chazey Partners

Organizational Cybersecurity

Chazey's Viewpoint

As incidents of cybercrime take precedence in the news and boardrooms, organizations globally are focusing on securing their positions. Most often this centers on technical solutions; hardware, software, and integrated tool sets. While technical solutions do have important roles in resilience, all too often they take center stage appearing as "silver bullet" solutions. The truth is that security, resilience, and assurance are founded on a solid operational infrastructure.

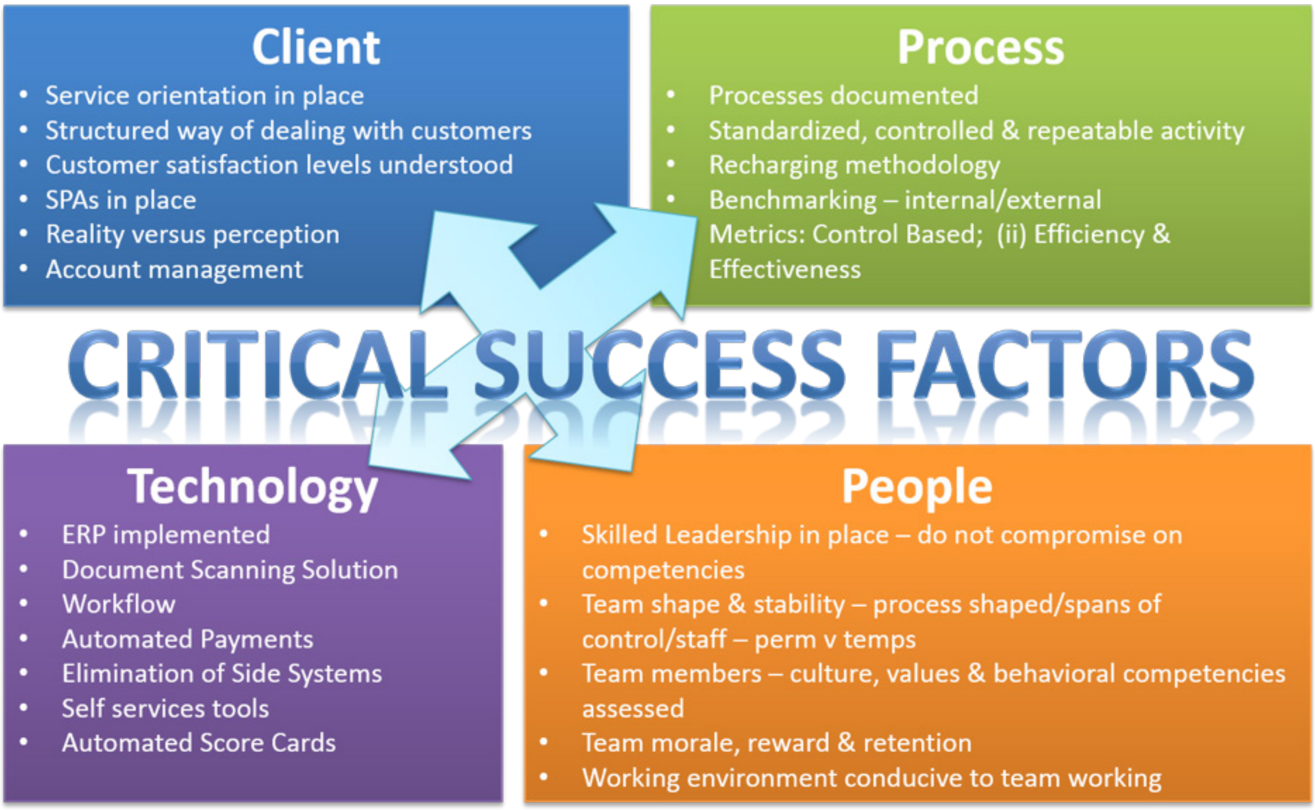
Technology is only one piece. Threats emerge and revolve on a number of fronts both from within and without of any organization. They adapt with advances in technology becoming more sophisticated in each iteration. Yet for even the most leading edge cybercriminals still rely on the basics; human weakness, bureaucratic process, and service culture. That is because cybercriminals know that organizations have interdependent dimensions. The weaker elements are exploited to overcome the strongest element. A chain is only as strong as its weakest link; technology is but a single link in the business operations framework.

Rob Serjeant
Cyber Security Practice Leader
Chazey Partners

Business Operations

In the hype over the technical developments and vulnerabilities, it is very easy to overlook the nuts and bolts of the matter to see what is really occurring. Cyber criminals are using technology to exploit the inner mechanisms of an organization to work against itself. They are forcing an organization to conduct improper transactions for criminal benefit. Money is being released for transfer / payment, network authorities escalated, data access protocols are engaged / over written, etc. The majority of instances are not crashing or destroying a system. Rather it is turning the system against itself, and it is done in such a way that the organization is unaware until a trap is sprung.

At Chazey, we define business operations as 4 equal and interdependent pillars that serve as the operational foundation of any organization. These are people, processes, client service, and technology (as shown in the figure below). Ideally all 4 should be managed in balance as they have a direct impact on one another. Over reliance or a singular focus on any one pillar compromises the integrity of the others as interdependence gives way to subservience. These are the weaknesses that cybercriminals are able to exploit through the use of technology.



Client

- Service orientation in place
- Structured way of dealing with customers
- Customer satisfaction levels understood
- SPAs in place
- Reality versus perception
- Account management

Process

- Processes documented
- Standardized, controlled & repeatable activity
- Recharging methodology
- Benchmarking – internal/external

Metrics: Control Based; (ii) Efficiency & Effectiveness

CRITICAL SUCCESS FACTORS

Technology

- ERP implemented
- Document Scanning Solution
- Workflow
- Automated Payments
- Elimination of Side Systems
- Self services tools
- Automated Score Cards

People

- Skilled Leadership in place – do not compromise on competencies
- Team shape & stability – process shaped/spans of control/staff – perm v temps
- Team members – culture, values & behavioral competencies assessed
- Team morale, reward & retention
- Working environment conducive to team working

Figure 1: 4 equal and interdependent pillars

Getting Back to Basics

A very basic tenant of assurance is “defense in depth”. In military terms, this means that fortifications, positions, and assets are deployed in a fashion that any one point of compromise is isolated so that it can be contained and addressed with supporting elements. No matter how vigilant or prepared one is, there is always a vulnerability that can emerge, even for a brief moment, where a compromise can occur. Defense in depth prevents it from escalating and expanding. The same applies to organizational resilience.

An example of this would be a breach of an employee's laptop. A cybercriminal using a fishing or spearfishing attack sends the employee an email with a link to malicious code. Essential security policy and practice dictates that an employee should never click on a link unless they are sure of its authenticity. However, through carelessness or inattention the employee clicks on the link. The workstation has been compromised and the organization is unaware.

At this stage the exposure is often very limited, but the threat has increased. A single workstation has little value on its own. The next stage is to expand the breach through escalated access to information or systems, or both. Internal requests are sent to expand the permissions to this end. Without defense in depth, the organization's transactional machinery can be used against itself. Seemingly legitimate requests are processed efficiently. The criminal then leverages the new permissions to expand in the network in a similar fashion below the radar. In a short amount of time, the compromise grows until the cybercriminal has achieved sufficient control to affect material damage.

A secure organization with defense in depth will have operational controls in place to detect and mitigate such expansion. Technology can certainly play a role in detecting anomalous patterns for investigation. But at the basic level operational controls can be even more effective. Permission requests should be reviewed, evaluated, and verified before any action is taken. Does the requestor have a defined business need for the escalated privileges? Is the request being made from a legitimate company terminal during normal operational hours for the person? How does it relate to past requests and work flows? These are essential front line considerations that seem logical and standard. But if trust is placed on the initial perimeter integrity so that internal requests are assumed to be legitimate they may be foregone. Further reliance on technology to 'detect' anomalous patterns outside of the operational considerations can compound the vulnerability. Well-structured attacks are hard to detect until a sufficient or identifiable activity has occurred and interdiction may not be real time. Thus, permissions may be granted and exploited before a response may occur.

Interdependence

In the previous example it is possible to see how the 4 pillars are germane to the problem of cybercrime. First there is technology, which was the initial point of compromise though ostensibly, it was in place and working properly. The real point to examine is how it facilitates the next phase of the compromise. Where requests are submitted through web portals the compromised laptop is used to submit an electronic request from a seemingly legitimate source. That is the process element, a normal and legitimate means to facilitate business needs. In this case it has been exploited for improper use. It then reaches a person to facilitate the request. This is where people and client service come into play in conjunction with process. Requests typically need to be processed in a prescribed manner for timeliness and efficiency. Is there a component to consider the appropriateness? Is there a meaningful verification step?

If a security component is not infused, then the machinery may simply respond to requests that are seemingly legitimate on the surface. What if there is no people component in this process? Perhaps there is an authentication requiring managerial approval. But what if this is also automated? If the manager's laptop has also been compromised or was the initial compromise, then used to ladder down to subordinates then the criminal is truly using the system against itself. A well-meaning organization with an expedient client focused process can quite easily be exploited.

Cybercrime is Human

No matter the technical dimension there is always a human element to cybercrime. Looking back to the 1990s, one of the most infamous hackers, Kevin Mitnic, perfected the use of 'social engineering' to facilitate his computer exploits. That is he learned how to talk to people in order to get them to disclose information and take actions that they should not have. By learning the processes, the organizational culture, and tapping into the client service / helpfulness focus, he turned the system against itself. More than 2 decades later, this technique continues to be commonly executed.

More recent high profile exploitations continue to leverage the good intentions of client-service focused employees. Cybercriminals call administrative staff impersonating executives in order to have them conduct inappropriate transactions. These range from resetting passwords so they can take control of computers to demanding payments be made immediately in order to save an important business deal. There is a human as the fulcrum to enact a process using technology while providing customer service. The pillars are taken out of balance so that supporting pillars become subservient, compromising the whole. Effective operational design with meaningful controls will inoculate an organization.

Even purely technical exploits, such as the SWIFT bank code scams and PIN readers are part of this dynamic. The transactions are leveraged entirely in the cyber realm but they pass through transactional gateways. The people, processes, and client service need to be brought in balance to shore up the inherent vulnerabilities of the technology. In each of these cases people did bring this to the forefront, noticing systematic errors in SWIFT for instance.

Balance

Good operational design infuses security protocols while facilitating effective business. Security should never stifle the flow of legitimate business. Controls must be rational and effective, with continuous improvement hardwired within the program. Business evolves as does cybercrime. So the operations must also evolve with the trends and techniques so the organization can operate efficiently with resilience.

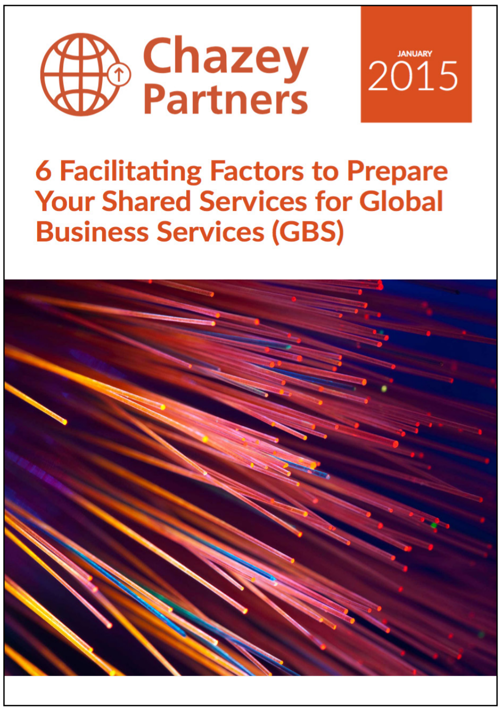
Furthermore, organizations need to take advantage of cybersecurity products and services within this framework. The key is choosing the right solutions that integrate with the overall operations to truly create defense in depth. No single product, service, or methodology will afford resilience on its own. That risks a single point of failure with the rapid evolution of cyber threats and the omnipresent human dimension. Technology always needs to be buttressed by the additional pillars of people, process, and client service.

About Chazey Partners' Cybersecurity Solutions

As a specialty advisory firm specializing in business transformation, Chazey Partners is uniquely positioned to partner with organizations globally to afford resilience in the face of cyber threats. Our professionals have on average 20 years of business experience with all facets of operations, specializing in transformation and shared services. Furthermore, we have members who have deep operational experience in security, organizational reliance, and business continuity. We afford this expertise to the benefits of our clients to ensure they have the right holistic solutions to operate effectively in light of the threats posed by cybercrime. For further information, please contact us and our practice leader Rob Serjeant based in Hong Kong (robserjeant@chazeypartners.com)

For more articles from Chazey Partners

Please visit www.ChazeyPartners.com/Resources or subscribe to our newsletters www.ChazeyPartnersInc.com/Subscribe



Chazey Partners

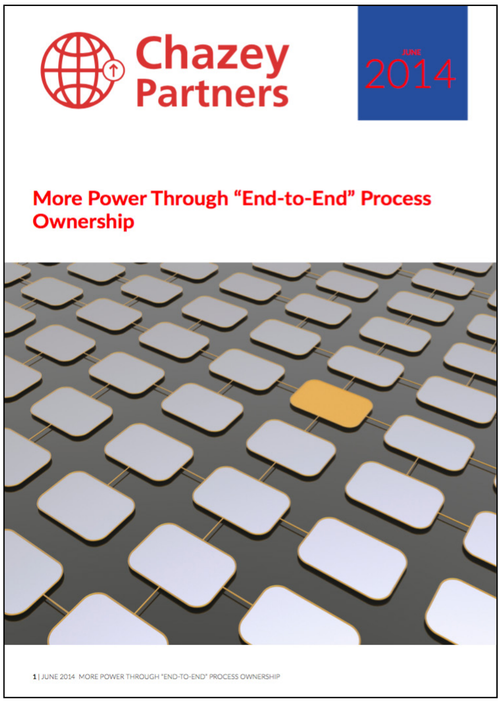
JANUARY 2015

6 Facilitating Factors to Prepare Your Shared Services for Global Business Services (GBS)

Preparing your shared services for Global Business Services

Over the past few years, although the Shared Services model has shown itself effective in delivering standardized, cost-effective, and consistent support services, evolving management thinking has led to a more pronounced demand for better quality data insights, more globalized support strategy, and integrated, enterprise wide decision-making that is leading many organizations to target a more sophisticated "global business services" model. In this article we highlight some of the "facilitation factors" that support a shift to GBS, and take a closer look at some of the characteristics that define successful Global Business Services models.

Click here to Read more



Chazey Partners

JUNE 2014

More Power Through "End-to-End" Process Ownership

1 | JUNE 2014 MORE POWER THROUGH "END-TO-END" PROCESS OWNERSHIP

More Power through Global End-to-End Process Ownership

While many organizations are already benefiting from Global Process Ownership, we are still seeing plenty suffer expensive mistakes that could be avoided. Read this report to find out how to drive more benefits across the end-to-end process.

Click here to Read more

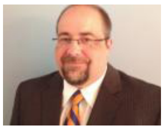
Chazey Partners Inc

Chazey Partners is a practitioners-led global management advisory business. We bring together a unique wealth of experience, empowering our clients to strive for world-class excellence through Business Transformation, Shared Services & Outsourcing, Technology Enablement, Process Enhancement and Corporate Strategy Optimization. We pride ourselves in having built, operated and turned around some of the world's most highly commended and ground breaking Shared Services Organizations, and for implementing many highly successful multi-sourced (shared services and outsourced) delivery solutions. Over the last 20 years, we have delivered numerous programs globally, in the US, Canada, UK, Continental Europe, Ireland, India, Eastern Europe, South America, Singapore, Australia, China, Middle-East and Africa. Our experience covers both Private and Public Sectors, providing expertise in a wide spectrum of business functions, including Finance, HR, IT and Procurement.

Learn more about us at www.ChazeyPartnersinc.com.

Phil Searle CEO & Founder
Chazey Partners
philsearle@chazeypartners.com

Chas Moore Managing Director, North America (West)
Chazey Partners
chasmoore@chazeypartners.com



Robert Towle Managing Director, North America (East)
Chazey Partners
roberttowle@chazeypartners.com

Esteban Carril Managing Director, Latin America
Chazey Partners
estebancarril@chazeypartners.com

Rob Serjeant Managing Director, Asia Pacific
Chazey Partners
robserjeant@chazeypartners.com