DTS DanTech Services
Computers under control!™

Technology Times June 2022 Issue

“With over 20 years of experience providing remote support to clients that rely on technology, I know what it takes to deliver business continuity. Add to that another 20 years of support in the service industry you’ll not find another company that takes customer service to heart as I do. Find out for your business what a difference it makes. “

What’s Inside:

Got IT Problem? - Click Here!

10 Reasons Why Change Fails

By Mark Sanborn

Jean-Jacques Rousseau said, “There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success than to take the lead in the introduction of a new order of things.”

Events, circumstances and forces beyond our control can impose change (and we’ve experienced a great deal of that these past few years), but what about the change programs you initiate? How successful are *you* at leading change?

How often have you seen efforts to create change stall? Ever been part of a team or an organization that attempted something really different and failed. We’ve all seen attempts at change bomb. What are the causes?

I spoken for and worked with over 3,000 organizations in my career. I’ve observed the successes and failures, and paid attention to what caused each. The following are some of the most common reasons I’ve identified why organizational change fails. You can use the list for diagnostic purposes, or to prevent mistakes in future attempts at change.

1. Mis-starts. A mis-start occurs when a change is ill-advised, hastily implemented or attempted without sufficient commitment. This is a leadership credibility killer.

It is often caused by a good idea that gains too much enthusiasm and too little examination. Change takes much organization effort, so be prudent in what you attempt.

- Continued on page 4

Lines of Business

Over the years, as technologies evolve and systems change, we have admittedly spread ourselves rather thin. Your business—and life—may somewhat resemble that statement! Because of this, we're looking at trimming down the outliers, chaff, and unproductive items we service. Some of this has been necessitated by our insurance carriers that wrap a policy or an exclusion around the services we provide. Our last assessment form was daunting, and then we were left playing catch up with their _*new*_ requirements—only to watch our insurance rates rise.

To those points, we've never filed a claim, nor have we had a reportable breach or compromise. The layers of security that we've used have been instrumental in protecting our client systems. And the realities are, something bad could have happened while I write this out. That's the world we now live in: things have changed. I'm sure you've seen it too.

We've developed a reliable, solid stack of services that protect our clients, such as our RMM (remote management & monitoring service) that aids us in protecting and maintaining servers and computers. That reboot request that you get? That's due to our vigilance in patch management. This is a key piece in the war against malware and cyber-attacks. Also key is the network infrastructure where your computers connect. We've partnered with Uplevel Systems & TransmosisOne to provide a modern, secure, upgradeable infrastructure that is all operational expense—no depreciation or future boat anchors, and fully supported with an upgrade path when required.

Our clients benefit from the services we provide. Protection of network, users, applications, and data are key to that protection. Layers of security that complement each other are crucial to protection. Keeping up with the evolution of system changes takes time, effort, and an understanding of the requirements needed. Things have changed. We are working at being proactive regarding the security needs of our clients. The needs of our business have changed. How have your business needs changed?

Policies That Can Save Your Business

Written or otherwise, businesses have policies in place for a multitude of reasons. Hiring, onboarding, time off, payroll, and sick leave are just a few of the common policies that most all companies have in place. What we're interested in are the items that may be neglected.

Does your business have the following policies in place?

Funds Transfer Policies:

A company's policy should state that any requests for the transfer of money that exceeds a certain dollar amount shall not be accepted by any request other than direct phone call or in person contact. This is especially important for C-Level, managers, and accounting—anyone that's authorized to request or accept these requests. Always take the extra steps needed to confirm a transfer request.

Account Information Change Policies:

Whether from employee, vendor, supplier, or any other partner, associate, or company, any requests to update banking or account information must be verified by either direct phone call or in person contact. Spoofed email or caller ID can look too real. A direct phone call should be from the accounting department—not to it. Other safeguards can also be implemented, such as dual-authorizations.

Acceptable Use Policy:

Every employee or contractor that uses the corporate or business network should have a signed AUP in their file. This policy should outline what's allowed or otherwise when using company resources, computers, networks, etc. It should cover BYOD (Bring Your Own Device) and Shadow IT (installing unauthorized applications or programs on a company computer).

Awareness & Training
Risk Assessment
Security Program
Managed Services
Policies & Procedures
Design & Implementation
Business Case

Cyber Incident Response Policy:

What is the policy of your company if the network or a computer is breached or compromised? Without a policy, how will you recover? Questions to be addressed: immediate response, notifications, triage, and investigation. This needs to be coordinated and implemented with your Managed Service Provider or IT tech support.

There are other policies that are protective of your business, yet the above recommendations are often overlooked. Each, though, has an important role regarding the protection of your business.

Why? *Because things have changed*. Cyber security risks have increased. Your business is under attack and risk mitigation, protection, and response are key to sustainability.

Do you know what your risks are? We can provide a CSRA (Cyber Security Risk Assessment) that can point out blind spots, areas needing adjustments, and recommendations on how to limit your risks. My calendar is at https://calendly.com/dts-danfoote. Schedule your CSRA with a two-hour block of time.

Dan

Shiny New Gadget Of The Month:

Eyoyo Underwater Fishing Camera Portable Video Fish Finder

Brand	Eyoyo
Model Name	EF09R-30
Power Source	Battery Powered
Screen Size	9 Inches
Display Type	LCD

9" LARGER COLOR MONITOR: The image display is more realistic and delicate. The 9 inches bigger TFT color monitor comes with a removable sun-visor ideal for bright environments.

1000TVL CAMERA w/ 12pcs INFRARED LIGHT: Specially manufactured 1000TVL program chip and 12pcs IR lights, fishes will be seen more clearly in the dark environment. Please note: the image will turn black and white if you open the infrared light.

DVR RECORDING FUNCTION: 8GB TF card included, you can record the underwater landscapes as your want.

SPECIAL FISH SHAPE AND SILVER COLOR DESIGN: This unique design will not disturb the fish, it can Lure the fish close to them.

6-8H WORKING TIME: 4500mAh high capacity rechargeable battery cell box included, It can also be used for light control.

How does network security work?

Network security combines multiple layers of defenses at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats.

How do I benefit from network security?

Digitization has transformed our world. How we live, work, play, and learn have all changed. Every organization that wants to deliver the services that customers and employees demand must protect its network. Network security also helps you protect proprietary information from attack. Ultimately it protects your reputation.

Types of network security

Firewalls. A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Intrusion prevention systems. An intrusion prevention system (IPS) scans network traffic to actively block attacks. Secure IPS appliances do this by correlating huge amounts of global threat intelligence to not only block malicious activity but also track the progression of suspect files and malware across the network to prevent the spread of outbreaks and reinfection.

Anti-virus and anti-malware software. "Malware," short for "malicious software," includes viruses, worms, Trojans, ransomware, and spyware. Sometimes malware will infect a network but lie dormant for days or even weeks. The best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.

Cloud security. Cloud security is a broad set of technologies, policies, and applications applied to defend online IP, services, applications, and other imperative data. It helps you better manage your security by shielding users against threats anywhere they access the internet and securing your data and applications in the cloud.

Data loss prevention. Organizations must make sure that their staff does not send sensitive information outside the network. Data loss prevention, or DLP, technologies can stop people from uploading, forwarding, or even printing critical information in an unsafe manner.

Email security. Email gateways are the number one threat vector for a security breach. Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send them to sites serving up malware. An email security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data.

Mobile device security. Cybercriminals are increasingly targeting mobile devices and apps. Within the next three years, 90 percent of IT organizations may support corporate applications on personal mobile devices. Of course, you need to control which devices can access your network. You will also need to configure their connections to keep network traffic private.

Web security. A web security solution will control your staff's web use, block web-based threats, and deny access to malicious websites. It will protect your web gateway on site or in the cloud. "Web security" also refers to the steps you take to protect your own website.

Backup, Disaster Recovery, and Cloud Mobility

When it comes to the IT data backup currently protecting your data—one of your company's most valuable assets—how much has changed over the last 35 years? Chances are that your process consists of backup virtual machines that, during off-peak hours, copy your data to a secondary backup location.

But when you back up data off-site, how well does that technology actually work? When a disaster happens, are you poised for a speedy and effortless disaster recovery? If your off-site backup solution doesn't offer continuous backup, it's not providing continuous data protection.

Continuous data backup is a fundamentally different and new technology sparking a growing shift—from recovery to availability, from restore to resume, from periodic to continuous.

The future of IT backup solutions is here, in a single, easy-to-implement solution that provides continuous data backup, speedy disaster recovery, and seamless cloud mobility.

"When Change Fails" - Continued from Page 1

2. Making change an option. When leadership commits to a change, the message must be that the change is not an option. Unfortunately the message that often comes across is "We'd really like you to change…" as if staying the same were an option. Whenever people have the option not to change, they usually won't. You need to make a compelling case for change and give people solid reasons for it. Don't allow commitment on the part of your team to be choice. If you've done your homework–and especially if you've considered your teams opinions and suggestions about the change–then moving forward is requirement for everyone.

3. A focus only on process. Leaders can get so caught up on planning and managing the process that they don't notice that no tangible results are being achieved. Leaders become more fixated on the process (which creates rigidity and prevents adjustments) than the results it was designed to create. The process needs milestones and measurable outcomes. If original plans aren't working, consider a revision, not of the change itself, but of the way you'll achieve it.

4. A focus only on results. This stems from a belief that the end justifies any means. Organizations tend to fail miserably in this regard: they downplay or ignore the human cost of change. It is this insensitivity to people's feelings that not only prevents the change but destroys morale and loyalty in the process. You can incur too much pain to make a change worthwhile, especially if it creates futility and despondency among employees or customers. Both need to believe the change is necessary and achievable. Pay attention not only to what people do but how they feel about the process.

5. Not involving those expected to implement the change (see #2). A great deal of resentment is aroused when management announces a change and then mandates the specifics of implementation without input from those doing the work. Employees need to be involved in two ways. First, their input and suggestions should be solicited when planning the change. Secondly, after a change has been determined, they should be involved in determining the means. Leadership needs to communicate, "Here's what must happen. How do you think it can best be done?"

6. Delegated to "outsiders". Change is an inside job. Although outsiders like consultants might provide valuable ideas and input, people inside the systems must accept responsibility for the change. Scapegoating and passing the buck is not an option, and often a reason outsiders are called in. It can be tempting to try to "buy" yourself a change, but it doesn't usually work.

7. No change in reward system. If you keep rewarding employees for what they've always done, you'll keep getting what you've always gotten. Make sure that rewards, recognition and compensation are adjusted for the desired change. And give special recognition to early adapters who help lead the change.

8. Leadership doesn't walk the talk. For change to happen, everyone must walk the talk but leaders must take the first steps. Change is aborted whenever leadership doesn't demonstrate the same commitment they expect from others. Grumbling behind the scenes and off-line comments that are negative easily undermine your attempt. People should be free to share ideas and opinions, but grumbling about a commitment that has been makes it sound like a false commitment.

9. Too little or too much. In this instance, the change is too massive to be achievable or too small to be significant. Like a good goal, a change program should be neither too easy nor too impossible. There is no algorithm to guide you here. A realistic assessment of your team's capacity and the time and money need for success is essential.

10. No follow-through. The best planning is worthless if not implemented, monitored and carried out. Responsibility must be clearly defined for making sure that follow-through is timely and intense. It is far easier to make plans than take action. Few skills are more important to effective leadership than the ability to change personally and the ability to lead others to change. When it comes to organizational change, beware these ten failure points.