5K TechnicalServices
ENHANCING PRODUCTIVITY, ONE CUSTOMER AT A TIME
ASSESS | ON-BOARD | MANAGE | PROTECT | OPTIMIZE

5K Technical Services
100 Allentown Parkway Ste 104
Allen, TX 75002
(469) 656-3159
info@5ktech.com
www.5ktech.com

5K Technical Services Presents:

Tech Times

Digital Transformation: Is Your Business Ready?

"Digital transformation" is a term likely circulating around IT departments everywhere. The vast majority of businesses today, no matter how big or small, will likely need to further digitalize their operations in order to keep up with competitive markets and an ever-growing list of digital trends. There are endless components associated with digital transformation. Late last year, tech company MuleSoft conducted their annual Connectivity benchmark for 2018, which surveyed more than 600 ITDM across a variety of industries. The results shed light on the importance of digital transformation, the issues that stand in the way of these transformations, and what ITDMs (Information Technology Decision Makers) believe to be the future of IT.

According to the survey, the stakes are high. The vast majority of ITDMs surveyed admitted their business's revenue would be negatively impacted if digital transformation didn't take place, and soon. Companies simply can't afford to let their IT operations fall to the wayside. Digitalizing your business operations is no easy task. Creating an online portal or creating new online processes doesn't mean you've digitalized. You've got to have clear goals before you begin this undertaking. More often than not, the top goal of businesses is to streamline their operations to run more efficiently.

Analyzing the Data
The vast majority of ITDMs understand the importance of upgrading their digital enterprises, with only 3% of organizations surveyed revealing they had no intentions of a digital revamp. In fact, approximately three quarters (74%) of those surveyed said they were currently undergoing digital transformation initiatives. Another 23% revealed plans to do so over the next three years.

Establishing Clear Goals
Digital transformations are futile without an end goal. Therefore, in order for ITDM to effectively transform their digital operations, they need to know both what is at stake, and in which ways they'd like a revamp to serve the organization.

Enhancing the Customer Experience
One other major goal for businesses undergoing digital transformation is to improve the customer experience. This means improving the customer experience by connecting customer-facing systems. The vast majority, 92% of ITDMs, revealed that forging a connected experience for both customers and employees is a priority for their respective organizations. As of December 2017, only 39% of those surveyed revealed their organizations offered a completely connected user experience.

Common Roadblocks
IT departments face a number of issues that hinder the potential for successful digital transformation. In addition to time constraints, there are other factors at play, such as misalignment between business and IT, problems within legacy infrastructure and systems, and a lack of resources and budget.

Digital transformations are a fact of life for many businesses today, and if they're not yet, they soon will be. From managing operations to improving customer and employee experiences, digital transformations are just one-way businesses are further embracing the power of the internet age.

Business Tech:

Should You Ban Laptops from Meetings?

Efficiency in the workplace is paramount to success. This concept is widely held across office environments everywhere. But while technology plays an increasingly valuable role in the way the world does business, that's not to say it doesn't come with its own unique set of drawbacks. Laptops and mobile devices are presenting problems within the workplace, particularly in regard to productivity.

In the workplace, screens often serve as barriers, and today's businesses are tasked with coming up with new ways to minimize these technological distractions. One effective method? Banning laptops from meetings.

The research is clear: laptops and mobile devices are no good for productivity, especially when it comes to meetings. Banning laptops and mobile devices from meetings can boost both productivity and efficiency. From reducing the amount of time it takes to conduct a meeting, to encouraging employees to be more present and engaged, banning laptops may be the next big trend in business.

The Dangers of Multi-Tasking
Technology that's been designed to improve our productivity can actually serve as culprits. They can interfere with our point of focus, whether that be our boss or colleague during an important meeting or a lecturer in the midst of a seminar. Laptops distract from learning, both for users and for those around them.

Research shows that multi-tasking is a killer of productivity. This doesn't apply to just individual productivity, either. It can also have negative effects on the organizational level, which is causing problems for businesses everywhere, regardless of industry. One report concluded that multitasking within organizations are even impacting the global economy, resulting in a loss of $450 billion.

The human brain simply does not retain information as well when there is a distraction like a laptop or mobile device competing for attention. There are numerous studies that back up these claims. In fact, when employees use their laptops or mobile phones during a meeting, they're known to do a number of things that hinder productivity, including asking questions that have already been answered. It may seem like nothing but a minor inconvenience to some, but gather enough instances like this, and you'll see how much time (and money) is at stake.

Not only is multi-tasking thought to hinder productivity, but it also makes employees more prone to distractions. Other negative effects include poor critical-decision-making and underperformance.

Benefits of The Ban
There are several benefits to banning laptops from meetings. From boosting creativity to cutting down on meeting time and even encouraging engagement, banishing laptops from the meeting room may be doing your company more good than you initially realize. This is why a growing number of managers are making the call.

Tips to Take Control
Once you've made the decision to ban laptops, you may want to put a solid system into place. Establishing a firm "no laptop" rule during meetings will help things remain consistent across the board. You may even consider a check-your-laptop-at-the-door rule that will help drive the point on home with your colleagues. If you are hosting a remote meeting where laptops are necessary, implement a rule that states all other apps and windows must be closed. This small step alone can help increase comprehension and cut down on distractions.

Online Marketing:

How Can You Stay Focused When You Have A "Million" Things To Do?

A compromised endpoint gives hackers everything they need to get a foothold in your security network. Once there, they can steal data and potentially hold it for ransom. That's why it's so important for business owners to secure their critical endpoints (including desktops, servers, and laptops). Otherwise, you could be leaving the front door wide open to hackers.

Today's attackers have learned how to bypass traditional antivirus software by using file-less attacks. These types of attacks can hide within sanctioned applications or even within the operating system. Even if you're vigilant about installing antivirus updates and patching, your organization may still be at risk.

What Are Endpoints?
Endpoints in networks are computer hardware items within the TCP/IP connections, which may include desktops, laptops, smartphones, tablet devices, printers, meters, terminals, smartphones and mobile devices, clients, and other forms of hardware.

Endpoint protection (EPP) has evolved to encompass code-based hacking, but the approach is often not adopted as organizations chose to use a legacy solution due to convenience or a lack of sufficient familiarity. Online sources including MSSP report this is common, but improvements in EPP will lead to more mainstream adoption. Meanwhile, current users may find that their existing network and operational variables demand some kind of improvement.

What Should I Know About Current Endpoint Security Risks?
One sign of a demand for improvement is continuing to use an antivirus program operating on a signature base. This form of technology is considered to be too slow to keep up with so-called 'zero day attacks,' or malware programs that are integrated with other coding.

Users should expect potential vulnerability with such programming, and devices that are not updated daily are considered vulnerable to ongoing malware threats. Additionally, signature sets (lists of operational protocol) can become so large that they run into the limit issue, leading legacy vendors to drop them, which creates a demand for new solutions that do not use signatures.

Ransomware, hacks designed to block user access until funds are provided to the hacker, has become increasingly destructive in the past few years. All it takes is one careless user who clicks on a link in an email, and your entire database could be locked until the ransom is paid.

Demands for improved management of antivirus software and continuing to use on-site antivirus management servers may also be grounds for improving EPP. You should be able to manage your entire antivirus system from your cloud, and if you cannot, you should consider updating and improving your system. Meanwhile, however, you should take care to ensure that any increased internet connectivity involved with a system improvement does not involve increased vulnerability. If you are able to manage your antivirus system from your cloud, but it does not seem to be sufficiently organized or efficient, you may benefit from substantial restructuring. Other practical reasons for investment in End Point Protection integrations or improvements include a developed distrust of your current system. Directly targeting EPP can be more efficient and effective.

If you are still doing regular background scans, or your new machines seem slower than you think they should be, you may want to consider improving your EPP. The newer generations of antiviral protection do not require background scanning. Traditional processes for security may be insufficient in addressing the range of possible endpoint attacks.

Technology @ Home:

How to Protect Your Child from Identity Theft

Depending on the age(s) of your child (ren), your response to this topic may be, "She's too young – she doesn't even have an identity yet."

Alas, not so. In our electronic society, kids exist in databases even before they're born. And they are an attractive target for several kinds of bad actors on the dark web – those who want to exploit their names and other data for identity theft, such as opening credit card accounts, child pornographers looking for images that can be photoshopped, school bullies, and so on.

Although this post focuses on identity theft, taking the steps described herein will also protect your children from other bad actors.

What's So Bad About Social Security Numbers?
As they were originally intended, nothing. The original intent was to use them to associate a specific individual with a specific record of earnings. But over the years, they morphed into the closest thing we have to a national identifier. Many organizations ask for it as a kind of reflex, with no intention of either using it or controlling its use. They have the notion that having an SSN makes your child a "real boy" (as opposed to a wooden one like Pinocchio?).

This leads to the first set of steps.
Get your child a Social Security Number. You will need it for some legitimate things about your child's identity, including passports. (Try taking the child abroad without one.)

Once you have it, put it in a safe place, like a bank safety deposit box. The same goes for birth certificates and other papers that identify your child. And of course, their passports

Never give anyone an SSN, or a copy of identifying documents, without knowing why they want it, and what the intended use is. If it is just a bureaucratic reflex, ask what you can do instead of handing it over.

Make sure the organization has a policy of destroying documents that are no longer needed. (This will guarantee a lot of comical blank stares.) The only acceptable responses are "we return them" or "we destroy them with a cross-cut shredder."

Monitoring Your Child's Financial Existence on The Web
Your child, from the moment of birth, is a thing that businesses highly value – a customer, even if it's you-by-proxy until your kid starts watching TV or using a computer or tablet. This means that your child will have an online existence from the moment of birth, and perhaps before. Those who exist can be exploited. So, you need to monitor your child's financial identity. This means:

Check your child's Social Security Earnings Record every year. You can get this by calling (800) 772-1213 or submitting SSA-7050 Form. If you know the child has never worked and you see any earnings, that is a sign of possible identity theft. Contact Social Security immediately. A list of Social Security local offices can be found here.

The same goes for earnings in excess of what you know a child who is working earned. A non-certified copy of the earnings record is free; a certified report is $34.00. There is no reason to get a certified copy just to monitor your child.

Check all three of your child's credit reports every year. Reports are free once per year. The three large credit bureaus that control most of the records are Equifax, Experian, and Transunion. Their online sites are Equifax, Experian, and Transunion.

Check any packages sent to your child. If you permit them to place orders online, make sure that what they got is what you or they ordered.

All these steps are relatively easy. The hardest part is teaching your child to be cautious (and safe) online. Social media are havens for identity thieves, and worse, predators. Teach your child to reveal private information only to trusted parties you have indicated that you approve of. For anything else, teach the child to respond with something like, "My parents don't want me telling that."

And, of course, it is obvious that you should keep your operating system, anti-virus, and anti-malware software updated. If you check every day, you will find that there is almost always an operating system patch, virus and malware definitions updates, or driver updates waiting to be installed.

Check to see if you can configure your OS and virus/malware software to update automatically. This exposes you to potential bugs, of course, but it will give you some peace of mind in the long run. Unless you are a true geek, consider it.

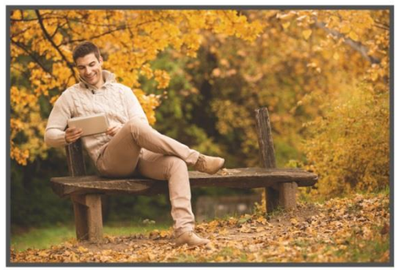
There are lots of other ways to keep your children safe online and this is an important topic you should discuss with them at the earliest time. You just can't wait until your kids are teenagers anymore to talk about cybersecurity and online predators.

November Special

Book Your FREE Dark Web Scan Valid Throughout November

SK TechnicalServices
ASSESS | ON-BOARD | MANAGE | PROTECT | OPTIMIZE

Call (469) 656-3159 or Email
info@5ktech.com
To Get Your Free Dark Web Scan.
Free until November 30.



Quotes of the Month

"If everything seems under control, you're not going fast enough."
Mario Andretti

"The greatest leader is not necessarily the one who does the greatest things. He is the one that gets the people to do the greatest things."
Ronald Reagan