Virtual DataWorks

TECH BYTES

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

INSIDE THIS ISSUE:

We love technology and we love helping people.

Give me a call today for a quick (non-salesy) chat to find out whether my team and I can help you better secure your data and get more out of your existing technology!

- **Matthew DeWees**
President

THE STATE OF RANSOMWARE 2024

Research has found that 99% of organizations affected by ransomware were successful in determining the primary cause of the attack.

Among the respondents, 34% attributed the root cause of the attack to email-based methods. Notably, a significantly higher number of incidents originated from malicious emails, which contained harmful links or attachments that facilitated malware downloads. In comparison, phishing attempts, which aim to deceive individuals into divulging sensitive information, accounted for roughly half as many incidents. It is important to recognize that phishing attacks are typically employed to acquire login credentials and subsequently serve as the initial stage of a compromised credentials attack.

Data Recovery

Nearly all organizations (98%) that experienced data encryption were able to recover their data. The two most common methods of data recovery were restoring from backups, which accounted for 68% of cases, and paying the ransom to obtain the decryption key, which accounted for 56% of cases. Interestingly, 26% of the organizations that encountered data encryption reported using alternative methods to retrieve their data. Although the survey did not delve into the specifics of these alternative methods, they may have involved collaborating with law enforcement or utilizing decryption keys that had already been publicly released.

Recovery Costs

Among different revenue segments, the lower and mid-revenue categories witnessed the most significant rise in overall recovery costs. Specifically, the cohort with revenue ranging from $250 million to $500 million reported the largest individual increase, amounting to $2 million. This represented a substantial jump from $885,018 to $2,885,296 in recovery expenses for organizations within this category.

Among the various revenue segments, organizations falling within the $1 billion to $5 billion revenue range witnessed a relatively modest increase of slightly over $400,000 in recovery costs. In contrast, the largest organizations with an annual revenue of $5 billion or more were the only cohort to observe a decrease in recovery expenses. Their costs decreased from $4,496,096 to $3,767,731, indicating a reduction in overall recovery expenditure for this particular group.

Analyzing the median recovery cost data validates the observed patterns. On a global scale, the median recovery costs have doubled, rising from $375,000 to $750,000 in the past year. The increases were primarily concentrated among the five lower revenue cohorts, which experienced significant cost escalations. In contrast, the recovery costs remained relatively stable for the two larger revenue cohorts.

Recovery Time: Impact of Backup Compromise

Multi-factor Authentication is a powerful tool that adds significantly to security. MFA users verify their identity through a secondary method such as a code sent to their mobile device. Enabling 2FA greatly reduces the risk of unauthorized access even if a hacker has compromised your password.

Stay Informed and Vigilant

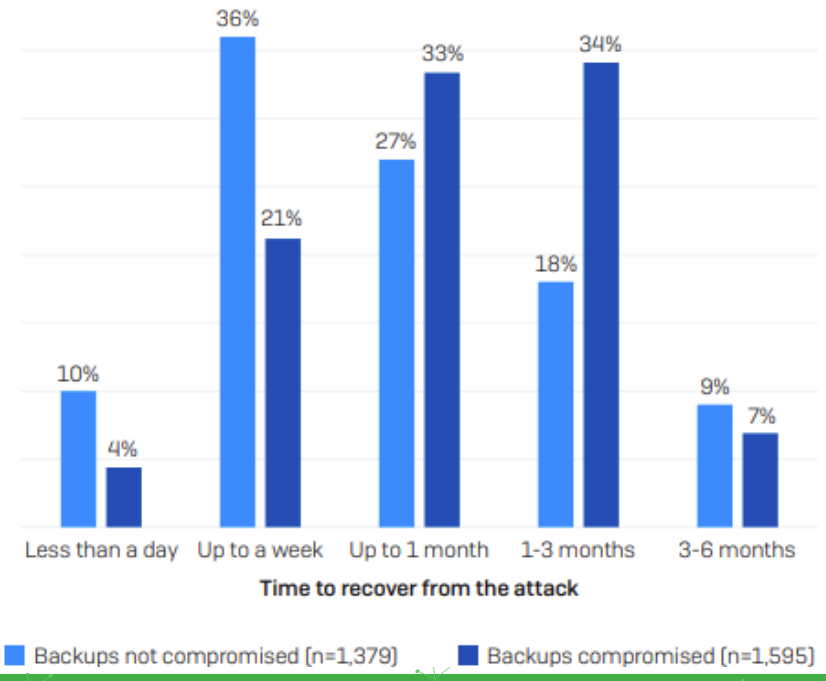
Be aware of the latest cybersecurity threats targeting the gaming community. Stay informed about potential risks as well as new hacking techniques and security best practices. Additionally, be vigilant when clicking on links or downloading files. Keep your guard up when interacting with unknown users within gaming platforms.

Keep Software and Antivirus Programs Updated

Regularly update your gaming platform, antivirus software, and operating system. This will patch vulnerabilities and protect against known exploits. Cybersecurity is an ongoing process. Staying up to date is crucial in thwarting potential attacks.

Use a Virtual Private Network (VPN)

Consider using a Virtual Private Network (VPN) to encrypt your internet connection. This enhances your privacy. It also adds an extra layer of protection against potential DDoS attacks as well as other malicious activities.



TOP DATA BREACHES OF 2023: NUMBERS HIT AN ALLTIME HIGH

The battle against cyber threats is an ongoing challenge. Unfortunately, 2023 has proven to be a watershed year for data breaches. Data compromises surged to an all-time high in the U.S.

The last data breach record was set in 2021. That year, 1,862 organizations reported data compromises. Through September of 2023, that number was already over 2,100.

In Q3 of 2023, the top data breaches were:

- HCA Healthcare
- Maximus
- The Freecycle Network
- IBM Consulting
- CareSource
- Duolingo
- Tampa General Hospital
- PH Tech

Let's look at the main drivers of this increase.

1. The Size of the Surge – Data breaches in 2023 have reached unprecedented levels. The scale and frequency of these incidents emphasize the evolving sophistication of cyber threats as well as the challenges organizations face in safeguarding their digital assets.

2. Healthcare Sector Under Siege – Healthcare organizations are the custodians of highly sensitive patient information. As a result, they've become prime targets for cybercriminals.

3. Ransomware Reigns Supreme – Ransomware attacks continue to dominate the cybersecurity landscape. The sophistication of this threat has increased.

4. Supply Chain Vulnerabilities Exposed – Modern business ecosystems have an interconnected nature. This has made supply chains a focal point for cyberattacks. The compromise of a single entity within the supply chain can have cascading effects.

5. Emergence of Insider Threats – The rise of insider threats is adding a layer of complexity to cybersecurity. Organizations must distinguish between legitimate user activities and potential insider threats.

6. IoT Devices as Entry Points – The proliferation of Internet of Things (IoT) devices has expanded the attack surface. There's been an uptick in data breaches originating from compromised IoT devices.

7. Critical Infrastructure in the Crosshairs – Critical infrastructure has become a target of choice for cyber attackers.

8. The Role of Nation-State Actors – Nation-state actors are increasingly playing a role in sophisticated cyber campaigns. They use advanced techniques to compromise sensitive data and disrupt operations.

9. The Need for a Paradigm Shift in Cybersecurity –The surge in data breaches underscores the need to rethink cybersecurity strategies.

10. Collaboration and Information Sharing – Collaboration among organizations and information sharing within the cybersecurity community are critical. Threat intelligence sharing enables a collective defense against common adversaries.

5 WAYS TO LEVERAGE MICROSOFT 365'S NEW AI INNOVATIONS

Microsoft 365 has been adding some amazing AI innovations. They sit inside tools like Word, Excel, PowerPoint, Teams, and more. These smart Copilot features can enhance your experience and boost productivity.

Here are ways to take advantage of the benefits offered by Microsoft Copilot.

1. Speed Up Document Creation
Copilot provides intelligent suggestions, helping you articulate your thoughts more effectively. It speeds up the writing process. It also ensures that your content is clear, concise, and tailored to your audience.

2. Enhance Your Teams Meeting Experience
Copilot in Teams can create coherent and context-aware responses. Such as a summary of meeting notes and an action item list.

3. Create PowerPoints with Ease
Become a "PowerPoint Master" with Copilot. The AI-infused features in PPT can create a slide deck for you based on text prompts, including the images.

4. Enjoy Smart Business Insights in Excel
Excel Ideas can automatically detect patterns and trends in your data. It will suggest charts, tables, and summaries that best suit your needs.

5. Save Time in Outlook with AI Help
Use Copilot in Outlook to summarize the key points of an email to save yourself reading time. It can also help write emails and suggest responses to emails in your inbox.

As we embrace the era of intelligent productivity, M365 becomes more powerful. Its new AI innovations pave the way for a more efficient work environment. Reach out to our team of IT consultants to learn how Virtual DataWorks can leverage technology to positively impact your business!

WAYS TO SHOW THE TANGIBLE VALUE OF CYBERSECURITY

The benefits of cybersecurity are often indirect and preventive in nature. This differs from tangible assets with direct revenue-generating capabilities.

Success is often measured by incidents that do not occur. This complicates efforts to attribute a clear monetary value. As a result, companies grapple with finding certain metrics.

Below are several ways to translate successful cybersecurity measures into tangible value.

- Quantifying Risk Reduction
- Measuring Incident Response Time
- Financial Impact Analysis
- Monitoring Compliance Metrics
- Employee Training Effectiveness
- User Awareness Metrics
- Technology ROI
- Data Protection Metrics
- Vendor Risk Management Metrics

READ MORE

9 TIPS FOR SETTING UP AI RULES FOR YOUR STAFF

Artificial intelligence (AI) is a powerful tool. It can enhance the productivity, efficiency, and creativity of your staff. But AI also comes with some challenges and risks. Businesses need to address and manage these to use AI effectively.

Here are some tips for setting up AI rules for your staff. These tips can help you harness the benefits of AI while avoiding the pitfalls.

1. Define the scope and purpose of AI use.
2. Establish ethical principles and guidelines.
3. Involve stakeholders in the decision-making process.
4. Assign roles and responsibilities.
5. Provide training and support.
6. Ensure data security and privacy.
7. Put a feedback loop in place.
8. Review and update your AI rules regularly.
9. Encourage a growth mindset.

READ MORE

EXPLORING WORKFORCE TECHNOLOGY MODERNIZATION FOR SMALL BUSINESSES

Technology plays a pivotal role in driving efficiency, productivity, and competitiveness. For small businesses, workforce technology modernization is both an opportunity and a challenge.

Embracing modern technology can empower small businesses. It can help them thrive in a digital era. Important benefits include improved employee retention and decreased cybersecurity risk not to mention the productivity and time-saving advantages.

Here are some steps to get your small business get started.

- Assess Your Current Technology Landscape
- Align Technology Goals with Business Objectives
- Focus on Cloud Adoption
- Invest in Collaborative Tools
- Look at Cybersecurity Measures
- Embrace Mobile-Friendly Solutions
- Look at Remote Work Options
- Consider Automation for Efficiency
- Provide Ongoing Training and Support
- Watch and Adapt to Evolving Technologies

EMBRACE INNOVATION, ELEVATE CARE

Are you ready to revolutionize the way you provide care in your nursing home? Technology is not just the future; it's the now. At Virtual DataWorks, we're committed to helping small businesses like yours thrive in the digital age.

Contact our skilled IT team today for a complimentary Network Assessment. Reach out to us now and take advantage of this valuable opportunity.

FOR MORE INFO. VISIT VIRTUALDATATWORKS.COM